
# NAVAL POSTGRADUATE SCHOOL

**MONTEREY, CALIFORNIA**

# THESIS

**DYNAMIC PERSONAL IDENTITY AND THE DYNAMIC IDENTITY GRID: HOW THEORY AND CONCEPT CAN TRANSFORM INFORMATION INTO KNOWLEDGE AND SECURE THE AMERICAN HOMELAND**

by

Ryan Burchnell

September 2008

| | |
|---|---|
| Thesis Advisor: | Anders Strindberg |
| Thesis Co-Advisor: | Richard Bergin |

**Approved for public release; distribution is unlimited**

THIS PAGE INTENTIONALLY LEFT BLANK

| REPORT DOCUMENTATION PAGE | | | Form Approved OMB No. 0704-0188 |
|---|---|---|---|
| Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503. | | | |
| **1. AGENCY USE ONLY** ***(Leave blank)*** | **2. REPORT DATE** September 2008 | **3. REPORT TYPE AND DATES COVERED** Master's Thesis | |
| **4. TITLE AND SUBTITLE** Dynamic Personal Identity and the Dynamic Identity Grid: How Theory and Concept Can Transform Information into Knowledge and Secure the American Homeland | | **5. FUNDING NUMBERS** | |
| **6. AUTHOR(S)** Ryan Burchnell | | | |
| **7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)** Naval Postgraduate School Monterey, CA 93943-5000 | | **8. PERFORMING ORGANIZATION REPORT NUMBER** | |
| **9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)** N/A | | **10. SPONSORING/MONITORING AGENCY REPORT NUMBER** | |
| **11. SUPPLEMENTARY NOTES** The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. | | | |
| **12a. DISTRIBUTION / AVAILABILITY STATEMENT** Approved for public release; distribution is unlimited | | **12b. DISTRIBUTION CODE** A | |


**13. ABSTRACT (maximum 200 words)**

Personal identification systems and processes; including those used for transliteration, travel visas and driver licenses; have failed to adequately adapt to the nation's new asymmetric threat. After September 11th, personal identification information about the attackers began to emerge and it became clear that it could have been used to identify the attackers prior to their terrorist acts. This study used qualitative research methods to construct meaning from previously uncorrelated issues and employed a three-stage analytical approach that grounded the research. The tertiary stage identified themes that had theoretical relevance and, in turn, a direct impact on the proposed solutions. The study borrowed concepts from a handful of formal qualitative methods; including grounded theory, content/document analysis, interviewing, triangulation and conceptual modeling. It found that ambiguity and ethnocentricity is inherent in American name-based identity collection practices, systems and processes; that consistently collecting specific name-based characteristics could be highly beneficial to combating terrorism; and that by leveraging the knowledge created by consistent collection practices, systems and processes we can transform name-based identity into a dynamic and leveragable commodity. To effectively do so, this project presents a substantive theory, *Dynamic Personal Identity,* and a conceptual technological system, the *Dynamic Identity Grid*, as potential solutions.


| **14. SUBJECT TERMS** Terrorism; Terrorist Travel; Kinship; Transliteration; Translation; Identity; Personal Identity; Arab Naming Conventions; Knowledge Flow; Intelligence and Security Informatics; ISI; Dynamic Personal Identity; DPI; Dynamic Identity Grid; DIG | | | **15. NUMBER OF PAGES** 130 |
|---|---|---|---|
| | | | **16. PRICE CODE** |
| **17. SECURITY CLASSIFICATION OF REPORT** Unclassified | **18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified | **19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified | **20. LIMITATION OF ABSTRACT** UU |

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release; distribution is unlimited**

# DYNAMIC PERSONAL IDENTITY AND THE DYNAMIC IDENTITY GRID: HOW THEORY AND CONCEPT CAN TRANSFORM INFORMATION INTO KNOWLEDGE AND SECURE THE AMERICAN HOMELAND

Ryan Burchnell
Major, Florida Highway Patrol
B.S., Florida State University, 1994

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2008**

Author: Ryan Burchnell

Approved by: Anders Strindberg, Ph.D.
Thesis Advisor

Richard Bergin
Thesis Co-Advisor

Harold A. Trinkunas, Ph.D.
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

# ABSTRACT

Personal identification systems and processes; including those used for transliteration, travel visas and driver licenses; have failed to adequately adapt to the nation's new asymmetric threat. After September 11th, personal identification information about the attackers began to emerge and it became clear that it could have been used to identify the attackers prior to their terrorist acts. This study used qualitative research methods to construct meaning from previously uncorrelated issues and employed a three-stage analytical approach that grounded the research. The tertiary stage identified themes that had theoretical relevance and, in turn, a direct impact on the proposed solutions. The study borrowed concepts from a handful of formal qualitative methods; including grounded theory, content/document analysis, interviewing, triangulation and conceptual modeling. It found that ambiguity and ethnocentricity is inherent in American name-based identity collection practices, systems and processes; that consistently collecting specific name-based characteristics could be highly beneficial to combating terrorism; and that by leveraging the knowledge created by consistent collection practices, systems and processes we can transform name-based identity into a dynamic and leveragable commodity. To effectively do so, this project presents a substantive theory, *Dynamic Personal Identity,* and a conceptual technological system, the *Dynamic Identity Grid*, as potential solutions.

THIS PAGE INTENTIONALLY LEFT BLANK

# TABLE OF CONTENTS

# LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| ACLU | American Civil Liberties Union |
| ANSI | American National Standards Institute |
| AQAM | Al Qaeda and Affiliated Movements |
| ARAN | Automatic Romanizer of Arabic Names |
| AUA | Automatic Understander of Arabic |
| CHDS | Center for Homeland Defense and Security |
| DAVID | Driver and Vehicle Information Database |
| DHS | Department of Homeland Security |
| DIG | Dynamic Identity Grid |
| DPI | Dynamic Personal Identity |
| EPIC | Electronic Privacy Information Center |
| ERRC | Eliminate--Raise--Reduce--Create |
| FBI | Federal Bureau of Investigation |
| GIG | Global Information Grid |
| HSPD | Homeland Security Presidential Directive |
| IAFIS | Integrated Automated Fingerprint Identification System |
| IP | Internet Protocol |
| ISI | Intelligence and Security Informatics |
| KM | Knowledge Management |

| | |
|---|---|
| NASCIO | National Association of State Chief Information Officers |
| NCIC | National Crime Information Center |
| NGA | National Geospatial Intelligence Agency |
| NSA | National Security Agency |
| OODA | Observe, Orient, Decide, Act |
| PDA | Personal Digital Assistant |
| TLO | Terrorism Liaison Officer |
| TOCA | Theory of Collaborative Advantage |
| TSC | Terrorist Screening Center |
| UAPI | University and Agency Partnership Initiative |
| US-VISIT | United States Visitor and Immigration Status Indicator Technology |

# ACKNOWLEDGMENTS

Thanks Be to God. Through God, All Things are Possible!

To My Wife Sarah: I am grateful and eternally indebted to you for your continued love and support in the face of weeks away from home, endless late nights, and weekends without me over the past eighteen months. Without you this project would not have been possible or worth the sacrifice.

To My Daughter Lyla: You will forever be my source of inspiration, strength and focus.

To My Daughters Kate, Jenna and Ally: Daddy loves you. I do not have any more homework to get in the way of our fun!

To Anders Strindberg and Richard Bergin: Your friendship, support, and professionalism got me through this project. Your brilliance, willingness to collaborate and thoroughness made this project great.

To Jennifer Glover and Jennifer Meaney: Your friendship and diligent efforts made the final product much better.

To Mark Nissen, Hsinchun Chin, Daniel Dolk and Richard Lutz: Your previous work and assistance throughout this project made my work easier and the results greater than I could have ever imagined.

To Executive Director Electra Bustle, Colonel John Czernis and Major Cyrus Brown: Your unfailing support made this project possible.

THIS PAGE INTENTIONALLY LEFT BLANK

# I. INTRODUCTION

Seven years ago, our nation began its day by reluctantly absorbing the most horrific attacks to occur on U.S. soil since Pearl Harbor. Scholars and practitioners immediately went to work in an attempt to stop international terrorism from reaching our shores again. One of the areas of greatest concern has been identifying who our enemies are and how to stop them. Countless testimonies, books and government reports call for our nation's officials to find new and clever ways to identify terrorists before their next strike. Some of the most compelling arguments to this end are found in the final chapters of the 9/11 Commission Report.[1] The final pages of this historic document call for the use of imagination in the development of programs and systems to combat terrorists and their organizations and to protect against terror attacks.[2] Most germane to this research project, the 9/11 Commission report calls for targeting terrorist travel, increased personal identity assurance, securing personal identification systems, and the construction of layered security systems.[3] The call for action on these items has led to imaginative programs and approaches that, for the most part, are disjointed, clumsy and fail to meet the demands placed on the system by their users and our new enemies. Many of them result in the wholesale dismissal of previous best practices, lessons learned and other expansions of knowledge. Our governmental organizations easily find themselves embroiled in perpetual knowledge revolutions, rather than meaningful knowledge growth.[4] Hsinchun Chen recently wrote:

> Current research on the technologies for counter-terrorism and crime-fighting applications lacks a consistent framework addressing the major challenges. Some information technologies including data integration, data analysis, text mining, image and video processing, and evidence

[1] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (Washington, D.C.: United States Government Printing Office, 2002), 567.

[2] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, 365-398.

[3] Ibid., 339-398.

[4] Thomas J. Housel and Arthur H. Bell, *Measuring and Managing Knowledge* (Boston: McGraw Hill, 2003), 162.

> combination have been identified as being particularly helpful. However, the question of how to employ them in the intelligence and security domain and use them to effectively address the critical mission areas of national security remains unanswered.[5]

This study attempts to solve the dilemma noted in Chen's research.

## A. PROBLEM STATEMENT

Globalization, multi-culturalism and technological innovation are facilitating our enemy's efforts to infiltrate our identification systems at a pace that far exceeds the nation's current capabilities. Innovations such as affordable laser printers, the internet and relatively cheap global air travel are just a few examples. Legacy identification related computer systems and governmental agency responsibilities such as visa and driver license issuance have failed to adequately adapt to the nation's new asymmetric threat. Policies, procedures, laws and documents are ethnocentrically structured and have failed to adapt to the global, multi-cultural world.[6] This research project attempts to take a strategic look at the problems associated with the personal identities of individual terrorists and those individuals that support terrorism. In the end, it will provide substantive theory and a conceptual framework aimed at solving some of the most compelling personal identity issues facing our nation.

The most horrific terrorist attacks in recent history have been connected to Al Qaeda and its affiliates.[7] Most of these terror attacks have been controlled from, planned or initiated in Middle Eastern countries and are predominately linked to perpetrators of Arab-Muslim descent.[8] As such, it is of great importance to accurately identify persons attempting to enter the United States from Middle Eastern countries or those wishing to

---

[5] Hsinchun Chen, *Intelligence and Security Informatics for International Security Information Sharing and Data Mining: Integrated Series in Information Systems*, vol. 10 (New York: Springer-Verlag), 182.

[6] See Chapter III.

[7] Anti-Defamation League, "Terrorism: Al Qaeda," http://www.adl.org/terrorism/profiles/al_qaeda.asp (accessed August 1, 2008).

[8] Karen DeYoung, "Letter Gives Glimpse of Al Qaeda Leadership," w*ashingtonpost.com*, October 2, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/10/01/AR2006100101083.html (accessed August 1, 2008).

enter the United States from other countries, but originating from an Arab-Muslim country. The technological systems used to verify and establish the personal identity of Arab-Muslim visitors to the United States are increasingly complex, and their application and use remain highly disparate throughout federal and state government.[9] The United States Government has been historically ineffective at consistently transliterating and collecting Arab-Muslim names and has not exhibited a clear strategic plan to change this mis-directed course of action in the future.[10] As a result, the U.S. has been equally ineffective at authenticating Arab-Muslim name-based identity and exploiting the genealogical characteristics of Arab-Muslim names in its counter-terrorism efforts.[11] These issues are the result of inconsistent practices for Arabic to English transliteration and the ethnocentric application of traditional American name structure to Arab-Muslim names during the collection process. The latter destroys the naturally occurring genealogical base found in Arab-Muslim names. The failure to collect all portions of Arab-Muslim names during the visa application and immigration processes may have directly led to failures in identifying familial links between persons that were known terrorist and those that were later identified as terrorists.

The inconsistent transliteration of Arab-Muslim names is most problematic when persons of Middle-Eastern and North African descent establish their official English language identity prior to entering, upon entering and/or while residing in the United States. For example, Mohamed Mohamed Amir Atta, a 9/11 hijacker, had a Florida Driver License issued under the name Mohamed Atta and used as many as seven other aliases while living in the United States.[12] It appears that his ability to do so was primarily due to inconsistencies in the transliteration and name collection processes that are currently in use throughout the United States' governmental bureaucracies.

---

[9] United States Department of Homeland Security, "Report Assessing the Impact of the Automatic Selectee and No Fly Lists," by Maureen Cooney, April 27, 2006.

[10] Sandra Rufolo, "Have We Got a Match for You," *ChannelWeb*, October 18, 2004, http://www.crn.com/government/50500044 (accessed August 1, 2008).

[11] Ibid.

[12] National Commission on Terrorist Attacks Upon the United States, *9/11 and Terrorist Travel: Staff Report of the National Commission on Terrorist Attacks Upon the United States*, by Thomas R. Eldridge, et al., (Washington, DC: Government Printing Office, 2004).

Additionally, eight of the nineteen 9/11 hijackers (42%) were genealogically related; however an exhaustive search of open source materials found no proof that they were linked by their familial ties while living in the United States prior to the 9/11 attacks.[13] According to an unidentified CIA report referenced in the *9/11 and Terrorist Travel Staff Report*, the "nineteen 9/11 hijackers used 364 aliases, including different spellings of their names and noms de guerre."[14] In addition, the report notes that Hesham Mohamed Ali Hedayet, also known as the "L.A. Airport Gunman," had State of California Driver Licenses issued in the name of Hesham Mohamed Hadayet and Hesham Mohamed Ali.[15] There are many other examples of familial links among individual terrorists and between individual terrorists and those persons that provide material support for their activities.[16] Chapter II will examine this issue in much greater detail.

The consistent rendition of Arabic names in English is difficult to accomplish due to competing theories and technological solutions. Competing theories are based upon longstanding research in the field of applied linguistics. Current technological solutions for the transliteration of Arab names derived from these theories have traditionally had no operating or algorithmic standards to ensure the consistency of the transliteration among the various systems. At the heart of these issues is partial name-based identity loss. The specific information that is lost in the transliteration and conformance process is unknown due to the lack of standards. The National Security Agency and National Geo-Spatial Intelligence Agency are currently involved in several research and development

---

[13] Sam Kharoba, "Understanding and Preparing for 21st Century Crime," *Social Security Administration*, www.ssa.gov/oig/investigations/PCIE-ECIE/presentations/Sam_Kharoba.pdf (accessed August 15, 2007).

[14] Eldridge, et al., *9/11 and Terrorist Travel*, 1-241.

[15] Ibid.

[16] "A Look at the Fort Dix Suspects," *Philadelphia Inquirer*, May 8, 2007, http://www.philly.com/philly/hp/news_update/20070508_A_look_at_the_Fort_Dix_suspects.html (accessed October 17, 2007); "Madrid Bombing Suspects," *BBC News*, http://news.bbc.co.uk/go/pr/fr/-/1/hi/world/europe/3560603.stm (accessed October 17, 2007).

programs and seem to be making significant technological advances in this area, but use of technological solutions for this issue remains highly disparate across federal and state governmental agency boundaries.[17]

The problems mentioned above most acutely present themselves in United States visa issuance and immigration procedures and their associated pre-printed or web-based forms. These modes of collection fail to accurately gather properly transliterated and formatted name-based identities from Arab-Muslim persons visiting or immigrating to the United States. The problems then manifest themselves in inaccurate official government documents such as travel visas and driver licenses. These official government identification documents perpetuate the existence of inaccurately transliterated and structured names. It appears that U.S. officials have taken an ethnocentric course of action in this regard, overlooking the basic principles of the Arabic language and Arab-Muslim culture to force compliance with American norms. By ethnocentric, it is meant that U.S. officials have developed forms, policies, laws, etc. that force the collection and perpetuation of personal names in the classic American style of First, Middle, Last. In doing so, the U.S. has likely lost crucial pieces in the terrorist identification puzzle, including genealogical information significant to counter-terrorism investigations and intelligence operations.

With each of these issues comes a realization that they are perpetuated by a host of inconsistent personal identification related governmental technological systems that are mis-aligned or not aligned at all. Even though great progress has been made to ensure a collaborative atmosphere throughout counter-terrorism related agencies of the U.S. Government, the technological systems that support them remain largely disjointed and cumbersome for their users. The ability of homeland security related governmental agencies to detect, deter, and protect the country against acts of terror is intimately tied to the technological capabilities of the agencies used to properly investigate, identify and

---

[17] "Aladdin Name Matcher – Name Matching by Normalization of Both Query and Data," *National Security Agency Central Security Service*, http://www.nsa.gov/techtrans/techt00066.cfm (accessed August 1, 2008) and http://www.nsa.gov/research/index.cfm; "NGA GEOnet Names Server," *National Geospatial Intelligence Agency*, http://earth-info.nga.mil/gns/html/index.html (accessed August 1, 2008) and http://www.nga.mil/portal/site/nga01/index.jsp?front_door=true (accessed August 1, 2008).

link terror suspects in advance of their acts. This includes the processes related to proper and consistent transliteration and collection of name-based personal identity characteristics.

## B. RESEARCH QUESTIONS

This study seeks to determine if Arab-Muslim visitors and immigrants to the United States are entering with ambiguous name-based identities or establishing them after entering the United States; if United States Government practices related to the collection of Arab-Muslim names and the establishment of associated personal identities appears to be ethnocentrically biased; and if substantive theory about the dynamics of personal identity and a conceptual integrated systems framework can be developed that are designed to mitigate the establishment of ambiguous name-based identities while ensuring personal privacy and providing an over-arching solution to enhance U.S. homeland security efforts.

## C. CHAPTER OVERVIEW

Chapter II is an extensive literature review designed to thoroughly discuss what is already known about the issues most closely related to the research. It discusses the importance of genealogy and name structure; the genealogical structure of Arab-Muslim names; the role of federal and state government in the personal identity process; the accurate rendition of Arab-Muslim names in English; the study of knowledge, knowledge flow, and knowledge management; link analysis and anomaly detection; decision support systems; and biometrics.

Chapter III discusses the research methodology, the data that was collected, the data analysis process, the specific research findings, the substantive theory developed and the conceptual framework proposed. In addition, it discusses other pertinent issues related to each of these items, recognizes the limits of the research and provides a strategy for further development and implementation of the conceptual framework.

Chapter IV discusses the specific conclusions and recommendations of the study and provides the author's thoughts about further related research.

# II. LITERATURE REVIEW & DISCUSSION OF KEY THEMES

The following chapter will review and discuss a wide range of literature in an attempt to provide context and meaning for the establishment of *Dynamic Personal Identity* (*DPI*) the *Dynamic Identity Grid* (*DIG*). *DPI* and the *DIG* are the deliverables of this project--they are designed to increase leveragable knowledge for homeland security practitioners and others concerned with personal identity. The literature focuses on a variety of areas that play a role in the name-based identity of Arab-Muslims entering the United States and other areas important to the development of *DPI* and the *DIG*. Specifically, the literature review focuses on the importance of genealogy and name structure; the genealogical structure of Arab-Muslim names; the role of federal and state government in the personal identity process; the accurate rendition of Arab-Muslim names in English; the study of knowledge, knowledge flow, and knowledge management; link analysis and anomaly detection; decision support systems; and biometrics. The author draws upon information from both theory and practice found in multiple literatures from several disciplines that are intimately related to personal identity. From the concepts discussed in the multiple literatures, the author is able to build a case for presenting substantive theory and a multidimensional framework to represent and visualize the information technology necessary to transform personal identity into dynamic, leveragable knowledge. The theory and framework provide the means to integrate the different perspectives from disparate literatures and will provide a guide for future research and design efforts. Both the substantive theory of *Dynamic Personal Identity* and the conceptual framework for the *Dynamic Identity Grid* are discussed in great detail in Chapter III.

## A. WHY FOCUS ON ARAB-MUSLIMS?

To explain why it is important to focus on persons of Arab-Muslim descent in this study a comparison of terrorist attack statistics found in the literature was completed. The comparison focused on Al Qaeda and the Irish Republican Army. Both terror organizations had multiple affiliated groups, which were also included in the review and

are noted appropriately below. The comparison found that the Irish Republican threat faced by the United Kingdom over the past few decades pales in comparison to the global Arab-Muslim threat that the U.S. faces today. The Irish Republican Army, the Continuity Irish Republican Army and the Real Irish Republican Army made up the core groups that the U.K. Government has fought against in Northern Ireland for decades. These groups have been found to include less than 1500 total members and have been involved in 139 attacks that have injured 217 persons and killed 66 others.[18] In comparison, Al Qaeda, the focus of the Global War on Terror, is believed by some to have more than 50,000 members.[19] A leading terrorism researcher contends that there are no known absolutes when discussing the membership size of Al Qaeda, but 50,000 members seems quite high.[20] In any case, the size of Al Qaeda is estimated to be much larger than 1,500. The group has been involved in 32 incidents that have injured 8,864 persons and have killed 3,464.[21] Although they have completed fewer attacks, they are much more deadly and have global reach capabilities.[22] In addition to the core Al Qaeda group, there are 37 other Islamic terrorist groups directly associated with Al Qaeda that have carried out an

[18] MIPT Terrorism Knowledge Base, "Irish Republican Army," http://www.tkb.org/Group.jsp?GroupID=55 (accessed February 24, 2008); MIPT Terrorism Knowledge Base, "Continuity Irish Republican Army," http://www.tkb.org/Group.jsp?GroupID=37 (accessed February 24, 2008); MIPT Terrorism Knowledge Base, "Real Irish Republican Army," http://www.tkb.org/Group.jsp?GroupID=91 (accessed February 24, 2008).

[19] MIPT Terrorism Knowledge Base, "Al Qaeda," http://www.tkb.org/Group.jsp?GroupID=6 (accessed February 24, 2008). The Congressional Research Service estimated the group's 1998 strength at 10,000 to 20,000 members, See: Kenneth Katzman, *CRS Report for Congress - Al Qaeda: Profile and Threat Assessment* (Washington, D.C.: Congressional Research Service, 2005), 14.

[20] Seth G. Jones, email interview with the author, August 10, 2008.

[21] MIPT Terrorism Knowledge Base, "Al Qaeda," http://www.tkb.org/Group.jsp?GroupID=6 (accessed February 24, 2008).

[22] Katzman, *CRS Report for Congress - Al Qaeda: Profile and Threat Assessment*, 14.

additional 1,167 attacks that have injured 12,079 people and have killed 6,215.[23] See Table 1 below for a further representation of this information.

| *Group* | *Number of Attacks* | *Injuries* | *Deaths* |
|---|---|---|---|
| Al Qaeda | 32 | 8864 | 3464 |
| Al Qaeda Related | 1167 | 12079 | 6215 |
| IRA | 139 | 217 | 66 |

Table 1. Al Qaeda versus Irish Republican Army

As depicted in the Table above, Al Qaeda and other affiliated groups - also known as Al-Qaeda and Affiliated Movements (AQAM) - represent a much greater threat than the Irish Republican Army and its affiliates. Without question, the Al Qaeda inspired "Jihad" against the West is a different kind of terrorist threat and one that is highly unique in our present time. The Al Qaeda attacks upon the United States of America on September 11, 2001 were an act of war and prove that Al Qaeda and its affiliates are not a mere criminal threat, but a highly effective asymmetric military threat. Open source information readily proves that they train militarily in rouge states and lawless areas across the Middle East.[24] The attacks on London on July 7, 2005 were a reminder that Al Qaeda and its affiliates maintain their ability to strike, even after being forced from the

[23] Follow individual group links from: "Al Qaeda Related Groups," MIPT Terrorism Knowledge Base, http://www.tkb.org/MoreRelatedGroups.jsp?groupID=6&pageIndex=0 and http://www.tkb.org/MoreRelatedGroups.jsp?groupID=6&pageIndex=1 (accessed February 24, 2008). Al Qaeda related groups include: Abu Hafs al-Masri Brigade • Ally, Abu Nayaf al-Afghani • Ally, Abu Sayyaf Group • Ally, Ansar al-Islam • Ally, Ansar al-Sunnah Army • Ally, Armed Islamic Group • Ally, Asbat al-Ansar • Ally, Battalion of the Martyr Abdullah Azzam • Ally, Eastern Turkistan Islamic Movement • Ally, Eastern Turkistan Liberation Organization • Ally, Egyptian Islamic Jihad • Ally, Eritrean Islamic Jihad Movement • Ally, Harakat ul-Mujahidin • Ally, Hizbul Mujahideen • Ally, Islamic International Peacekeeping Brigade • Ally, Islamic Jihad Group • Ally, Islamic Movement for Change • Suspected Alias/Ally, Islamic Movement of Uzbekistan • Ally, Jaish al-Taifa al-Mansoura • Ally, Jaish-e-Mohammad • Ally, Jemaah Islamiya • Ally, Lashkar-e-Taiba • Ally, Laskar Jihad • Ally, Libyan Islamic Fighting Group • Ally, Moroccan Islamic Combatant Group • Ally, Pattani United Liberation Organization • Ally, Riyad us-Saliheyn Martyrs' Brigade • Ally, Takfir wa Hijra • Shared Members, Taliban • Ally, Tawhid and Jihad • Ally, Tunisian Combatant Group • Ally, al-Gama'a al-Islamiyya • Ally, al-Islambouli Brigades of al-Qaeda • Supported Cause, al-Ittihaad al-Islami • Ally, al-Qaeda Organization in the Islamic Maghreb • Ally, al-Qaeda Organization in the Land of the Two Rivers • Ally, al-Qaeda in the Arabian Peninsula • Ally.

[24] Agence France-Presse, "More foreign fighters move into Pakistan's tribal areas, report," *AFP.com*, July 10, 2008, http://afp.google.com/article/ALeqM5hNzXPQQNbA3bRiC7nLUeyTyPbqSg (accessed August 1, 2008).

cities of Afghanistan into the Pashtun Tribal Areas near the Pakistani border.[25] Within the tribal areas, Al Qaeda has maintained and strengthened its global network and appears to be capable of mounting attacks for the foreseeable future.[26] In fact, Al Qaeda "has revitalized itself and returned to the operating style it enjoyed prior to 9/11," therefore it is important to continue a strong focus on Arab-Muslims that wish to do harm to the United States.[27]

## B. WHY GENEALOGY AND KINSHIP ARE IMPORTANT

Seven of the nineteen 9/11 hijackers were, among other personal characteristics, genealogically related; however, an exhaustive search of the literature found no proof that they were linked by their familial ties while living in the United States prior to the 9/11 attacks.[28] Genealogy is a consistent factor in the makeup of terror cells and groups. In a recent book, Barry Cooper stated, "With criminal and terrorist networks, trust is often enhanced by blood and brotherhood, that is, by kinship, marriage and shared experiences."[29] However, kinship being a central theme in social networks is not limited to criminal and terrorist enterprise. It has been found to be a part of other groups at the edge of society, including religious cults and sects.[30] Research into the impact of kinship on religious cults and sects found that kinship is central to the structure of these groups

---

[25] Paul Reynolds, "Bomber video 'points to al-Qaeda'," *BBC.com*, September 2, 2005, http://news.bbc.co.uk/2/hi/uk_news/4208250.stm (accessed August 1, 2008).

[26] J. Michael McConnell, *Annual Threat Assessment of the Director of National Intelligence* (Washington, DC: Office of the Director of National Intelligence, 2008), .6; The Boston Globe, "Pakistan tribal area called likely source of next attack on the U.S.," *boston.com*, June 11, 2008, http://www.boston.com/news/world/articles/2008/06/11/pakistan_tribal_area_called_likely_source_of_next_attack_on_us/ (accessed August 1, 2008).

[27] Seth G. Jones, *Getting Back on Track in Afghanistan* (Santa Monica, CA: RAND Corporation, 2008), 5.

[28] Kharoba, *Understanding and Preparing for 21st Century Crime*.

[29] Barry Cooper, *New Political Religions* (Columbia: University of Missouri Press), 158-170.

[30] Rodney Stark and William Sims Bainbridge, "Networks of Faith," *The American Journal of Sociology* 85, no. 6 (May 1980): 1376-1395; John Lofland and Rodney Stark, "Becoming a World Saver: A Theory of Conversion to a Deviant Perspective," *American Sociological Review* 30, no. 6 (December 1965): 862-875.

and to preventing defection.[31] It is the recognition of the pervasive nature of kinship ties within and between terror groups that is most important to this study.

Further review of the literature and other open source information indicates that there is strong evidence of significant familial links among individual terrorists and in the connections between terror groups.[32] A Staff Report of the National Commission on Terrorist Attacks Upon the United States, the 9/11 Commission Report, and multiple newspaper articles and websites clearly establish significant genealogical links between individual terrorists involved in various attacks around the globe and, to a slightly lesser degree, they provide evidence of genealogical links between terrorists and those who support their activities.[33] Marc Sageman discusses the significant role that kinship played in the terrorist activities of Ramzi Yousef, the 1993 World Trade Center Attack mastermind.[34] Simon Reeve describes how Ramzi Yousef recruited his own father and one of his brothers for a terror attack deep inside Iran.[35] One of the planners of 9/11, Khalid Shaikh Mohammed, is Ramzi Yousef's Uncle.[36] Mohammed's brother worked with jihadist Ahmed Said Khadr in Peshwar in the mid-80s.[37] Khadr's sons Abdallah,

---

[31] Stark, "Networks of Faith," 1376-1395.

[32] Hamied N. Ansari, "The Islamic Militants in Egyptian Politics," *International Journal of Middle East Studies* 16, no. 1 (March 1984): 123-144; Saad Eddin Ibrahim, "Anatomy of Egypt's Militant Islamic Groups," *International Journal of Middle East Studies* 12, no. 4 (December 1980): 423-453; Saad Eddin Ibrahim, "Egypt's Islamic Militants," *MERIP Reports* 103 (February 1982): 5-14; Marc Sageman, "Understanding Jihadi Networks," *Strategic Insights* IV, no. 4 (April 2005), http://www.ccc.nps.navy.mil/si/2005/Apr/sagemanApr05.asp (accessed August 1, 2008); Dan Murphy, "How Al Qaeda Lit the Bali Fuse," *Christian Science Monitor*, June 19, 2003; Danish Ministry of Justice, *Recruitment of Islamist Terrorists in Europe*, by Michael Taarnby (Aarhus: University of Aarhus, 2005), 56.

[33] *9/11 and Terrorist Travel*, 1-241.; Alice Falk, ed., *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, 1-277; Context of 1980s and 1990s: Most 9/11 Hijackers Have Middle-Class Backgrounds, see Center for Grassroots Oversight, http://www.cooperativeresearch.org/context.jsp?item=a80s90smiddleclass (accessed August 15, 2007); Andrew Selsky, "Pentagon Releases Gitmo Detainees' Names," *Washington Post*, May 15, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/05/15/AR2006051500905_2.html (accessed September 1, 2007); Asla Aydintasbas, "Putting it All Together," *The Opinion Journal – Wall Street Journal Online*, August 21, 2002, http://www.opinionjournal.com/editorial/feature/.html?id=110002160 (accessed August 31, 2007).

[34] Sageman, *Understanding Terror Networks*, 109.

[35] Reeve, *The New Jackals*, 66.

[36] Bongar et al., *Psychology of Terrorism*, 56.

[37] Sageman, *Understanding Terror Networks*, 112.

Abdel Rahman, and Omar have also been linked to terrorism.[38] Hamburg Cell member Ramzi bin al-Shibh was the cousin of 9/11 co-terrorist Kalid al Midhar's wife.[39] The Gufron brothers--Ali, Amrozi, Ali Imron and Ali Fauzi--were involved in the Bali nightclub bombings.[40] The millennium plot and the 9/11 attack included two sets of brothers, and the 9/11 attacks also included groups of cousins.[41] The Madrid bombings in 2004 were carried out by an operational group that included two brothers, Mohannad and Moutaz Allmalah Dabas.[42] More recently, the Fort Dix Terror Plot in 2007 included three brothers, which made up half of the terror cell.[43]

The familial link between terrorists and their supporters seems to be nearly as strong as it is between individual terrorists, making it an important consideration. For example, the descendants of King Faisal of Saudi Arabia (1964-1975) are allied closely with, but are not directly related to, Osama bin Laden.[44] However, this group of Saudi Royal supporters fully supports bin Laden and his group Al Qaeda. Prince Turki al Faisal was the Saudi Director of Intelligence until August 2001.[45] Turki is known for his support of Al Qaeda.[46] Turki's brothers are also deeply ingrained in Saudi politics; one being the head of a philanthropic organization originally headed by bin Laden himself and another served as the Saudi Foreign Minister.[47] Mohammed Jamal Khalifa, Osama bin Laden's brother-in-law, had a number of businesses that supplied direct financial and logistical support to Abu Sayyaf, the Armed Islamic Group in Algeria and the Moro

---

[38] Sageman, *Understanding Terror Networks*, 112.

[39] Ibid., 110.

[40] Ibid., 112.

[41] Ibid.

[42] Javier Jordan, Fernando Manas and Nicola Horsburgh, "Strengths and Weaknesses of Grassroots Jihadist Networks," *Studies in Conflict and Terrorism* 31, no. 1 (January 2008): 17-39.

[43] Staff Writer, "A Look at the Fort Dix Suspects," *Philadelphia Inquirer*, May 8, 2007.

[44] David Wurmser, "The Saudi Connection," *The Weekly Standard*, vol. 7, no. 7, October 29, 2001, 15.

[45] Ibid., 15.

[46] Ibid.

[47] Ibid.

Islamic Liberation Front.[48] The widow of 7 July London bomber Mohammed Sidique Khan and her brother were arrested in May 2007 for helping prepare and instigate acts of terror.[49] This London trend repeated itself when brothers of two of the would-be 21 July London bombers were arrested for supporting their kin after the attack failed.[50] When questioned about the 1993 World Trade Center bombing, Ramzi Yousef told Joint Terrorism Task Force Agents that he had received financial support from family and friends for the attack.[51] Yousef's Uncle, Zahid Al-Shaikh, ran a Saudi charitable organization known to support veterans of the Afghan war and is a known confederate of Osama bin Laden.[52] Yousef also received support from a host of family members that moved to the Philippines after the 1993 World Trade Center attack, to include a younger brother and distant cousin.[53] It is even thought, but as of yet unproven, that Yousef met with Oklahoma City bomber Terry Nichols in Cebu City in late 1994 to discuss bomb making.[54] The two allegedly met through Nichols' Filipino wife.[55] Nichol's wife was born in Cebu City and has links to radical Muslim extremists in the area. [56] The Madrid bombings were heavily supported by two different families. The two groups include six persons from a single family, including two bothers, their parents, and two of their uncles.[57] The other family group that supported the Madrid bombings, the Akcha family, included three siblings, a female and her two brothers.[58] The nephew of Kalid Sheikh

---

[48] David Martin Jones, Michael L. R. Smith, and Mark Weeding, "Looking for the Pattern," *Studies in Conflict and Terrorism*, 26 (2003): 443-457.

[49] Sandra Laville and Vikram Dodd, "Widow of July 7 Attacks Ringleader Held," *The Guardian*, May 10, 2007.

[50] "Five Jailed for Assisting Terrorists," London Metropolitan Police Service, http://cms.met.police.uk/met/layout/set/print/content/view/full/10459 (accessed February 14, 2008).

[51] Reeve, *The New Jackals*, 108.

[52] Ibid., 48.

[53] Ibid., 73-74.

[54] Ibid., 82-83.

[55] Ibid., 83.

[56] Ibid.

[57] "Madrid Bombing Suspects," *BBC News*, http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/1/hi/world/europe/356 (accessed October 18, 2007).

[58] Ibid.

Muhammad, Ammar al Baluchi, was responsible for providing a majority of the funding for the 9/11 hijackers once they entered the United States.[59] In addition, Baluchi's sister is married to 1993 World Trade Center mastermind Ramzi Yousef.[60]

Within the Arab World, the reliance on kinship as a precursor to group membership is a centuries old practice. According to Ayla Schbley, "Hizbullah is organized in cells; each cell is a group of four to eight Muslim Shi'a elements tightly knit by blood. Family ties engulf Hizbullah's cells with the needed security."[61] He goes on to say "Kinship is and has always been the glue that protects each Hizbullah cell from mutation and disassociation."[62] The kinship ties within terrorist organizations are deeply rooted in centuries old tribal affiliations prevalent throughout the Middle East, where trust and status are determined by familial affiliation, not personal reputation. The prime example of tribal affiliation and its related impact on group affiliation can be found within the Afghan Taliban, where eight of the top eleven senior leaders are from the Ghilzai area and all but one of those are from the Hotaki Tribe.[63] Kinship ties within terrorist groups extend beyond Al Qaeda and other Islamic terror groups. Donatella della Porta concluded that many of the terrorists included in her study of Italian left-wing terrorists had at least one relative that shared their commitment.[64] It is one of Sageman's conclusions that, due to the deep kinship ties within terrorist organizations, the relatives of identified terrorists need to be pursued and investigated wherever they reside.[65] In fact, research has shown that kinship is not only a major factor of membership within terrorist

---

[59] National Commission on Terrorist Attacks upon the United States, *Monograph on Terrorist Financing*, by John Roth, Douglas Greenberg and Serena Wille, (Washington, DC: USGPO, 2003), 152.

[60] National Commission on Terrorist Attacks upon the United States, *Monograph on Terrorist Financing,* 134.

[61] Ayla Hammond Schbley, "Torn Between God, Family, and Money," *Studies in Conflict and Terrorism*, 23 (2000): 175-196.

[62] Schbley, "Torn Between God, Family, and Money," 187.

[63] Thomas H. Johnson and M. Chris Mason, "Understanding the Taliban and Insurgency in Afghanistan," *Orbis* 51, no. 1 (Winter 2007): 71-89.

[64] Donatella della Porta, "Recruitment Processes in Clandestine Political Organizations, *International Social Movement Research*, 1, 155-165.

[65] Sageman, *Understanding Terror Networks*, 178.

cells and organizations, but also across organizational boundaries.[66] Sageman contends that kinship ties extend well beyond brothers and cousins and includes in-laws and spouses – "Marriage exposes people to new kinship and friendship networks, which may inspire affiliation with the jihad."[67] In fact, most terrorists have become members of a terrorist organization through relatives with the number of couples and brothers/sisters being very high.[68] The Jamaat al-Muslimin, the Egyptian-based forerunner to Al Qaeda, relied heavily on kinship in their recruitment efforts.[69] In Southeast Asia, the role of kinship remains strong and is considered by some researchers as the glue that holds radical networks together in that part of the world.[70] This suggests that genealogical links between individual terrorists are both important and occur frequently enough to be a significant factor in U.S. counter-terrorism efforts.

Attempting to list all of the potential familial ties between individual terrorists and those that support them is an endless quest and likely the subject matter for another study. However, this study has tried to explain some of the most intriguing aspects of this phenomenon in order to set the stage for the rest of this project and for validating the reasons for its conclusions. Based on the literature and a thorough examination of open source materials regarding several high profile terror attacks, it is clear that genealogy is an important investigative factor that may lead to the identification, defeat and/or apprehension of individual terrorists and those that support them. In fact, after 9/11 it was found that all nineteen hijackers were within two steps of the original suspects identified in 2000, well before the attacks occurred.[71]

---

[66] Magouirk, "Connecting Terrorist Networks," 12.

[67] Sageman, *Understanding Terror Networks*, 113.

[68] Ibid., 131.

[69] Saad Eddin Ibrahim, "Anatomy of Egypt's Militant Islamic Groups," *International Journal of Middle East Studies*, 12, 423-453.

[70] Justin Magouirk, Scott Atran and Marc Sageman, "Connecting Terrorist Networks," *Studies in Conflict and Terrorism* 31, no. 1 (January 2008): 1-16.

[71] Valdis Krebs, "Connecting the Dots," *Social Network Analysis Website*, http://orgnet.com/tnet.html (accessed January 15, 2008).

## C. WHY THE STRUCTURE OF ARAB-MUSLIM NAMES IS IMPORTANT

As discussed by Salih and Bader, western cultures do not regularly base personal names on genealogy.[72] They conclude that personal names have no particular significance in western society, and that they do not regularly relate to the condition or attributes of the bearer, his family or his environment.[73] In contrast, "The Arabic naming system does not conform to the English system."[74] In fact, Notzon and Nesom contend that "the Arabic system has a regularity of its own…related to country of origin, religion, culture, level of formality and even preference."[75] There is strong evidence that a genealogically-based Arab-Muslim name structure exists. The extent to which the structure is readily used is much less clear. However, knowledge of the structure and its historical use, discussed in detail by Beeston, should allow for an easy transition to procedures that collect this information.[76] The publication, "A Guide to Names," distributed by Interpol states that a genealogically-based name structure exists in the Arabic speaking countries of Saudi Arabia, the United Arab Emirates, Yemen, Oman, Kuwait, Bahrain, Qatar, Iraq, Lebanon, Syria, Jordan, Egypt, Mauritania, Sudan, Libya, Tunisia, Algeria, and Morocco.[77] According to Schimmel, full Arabic names consist of five parts--the *ism, kunya, nasab, laqab* and *nisba*--all of which are genealogical indicators. [78] This same structure is discussed in detail by Notzon & Nesom, Richards,

---

[72] Mahmud Husein Salih and Yousef T. Bader, "Personal Names of Jordanian Arab Christians: A Sociocultural Study," *International Journal of Social Language,* 140 (1999): 29-43.

[73] Ibid.

[74] Beth Notzon and Gayle Nesom, "The Arabic Naming System," *Science Editor*, 28, no. 1 (January/February 2005): 20-21.

[75] Ibid.

[76] A.F.L. Beeston, *Arabic Nomenclature: A Summary Guide for Beginners* (Oxford: Oxford University Press, 1971), 8.

[77] UK Government and Interpol, *A Guide to Names and Naming Practices*, Anonymous (London, UK Government Press, 2006), 88.

[78] Annemarie Schimmel, *Islamic Names*, (Edinburgh: Edinburgh University Press, 1989), 1-13.

Beeston, and Appleton.[79] United States Foreign Affairs Manual Volume 9, Appendix F also discusses Arab-Muslim name structure in the format described here.[80] Based on the literature, it is fair to conclude that the standard, four part Arab-Muslim name is rich in genealogical information and that the four part name consists of the *ism* (given name), the 1st *Nasab* (Father's *Ism*), the 2nd *Nasab* (Paternal Grandfather's *Ism*) and the *Hisba* or *Nisba* (Family or Tribal name).[81] (See Figure 1 – Standard Arab-Muslim Name Structure)

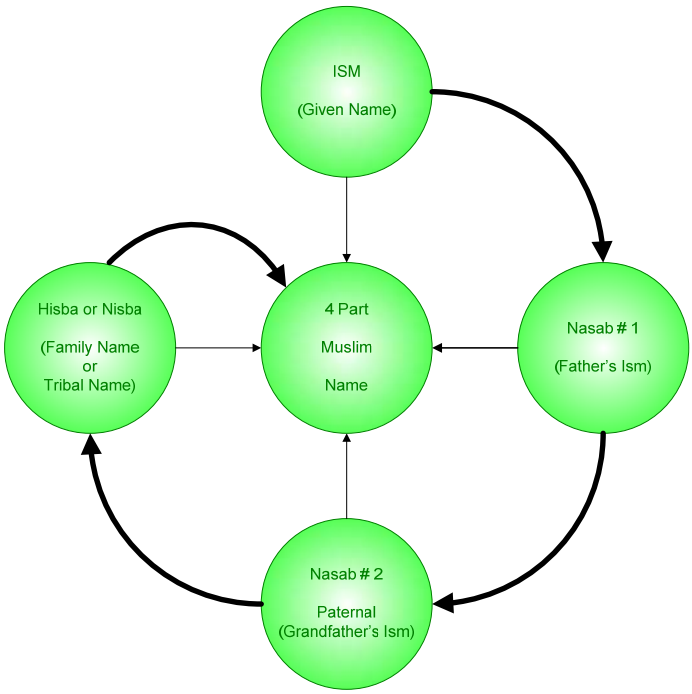


Figure 1. Standard Arab-Muslim Name Structure

[79] Notzon and Nesom, "The Arabic Naming System," 20-21.; James Richards, "Know Your Customer: Naming Conventions for Arabic, Russian, Chinese, Vietnamese, West African and Hispanic Cultures" (Oklahoma City: Bankers Online), http://www.bankersonline.com/tools/namingconventions.pdf (accessed August 10, 2007); Beeston, *Arabic Nomenclature,* 1-8.; David B. Appleton, "Period Arabic Names and Naming Practices," *The Society for Creative Anachronism*, (2003), http://heraldry.sca.org/laurel/names/arabic-naming2.htm (accessed July 24, 2007).

[80] United States Department of State, *Foreign Affairs Manual Volume 9* (Washington, DC: United States Government Printing Office, 2008), http://www.state.gov/m/a/dir/regs/fam/c22167.htm (accessed November 18, 2007).

[81] Annemarie Schimmel, *Islamic Names* (Edinburgh: Edinburgh University Press, 1989), 1-13.

## D. WHY GOVERNMENT IS IMPORTANT IN THE PERSONAL IDENTITY PROCESS

In 2006, the United States Department of State issued over 5.8 million non-immigrant visas, granting foreign citizens the right to enter the United States legally.[82] There were over 2.2 million non-immigrant visas issued to residents of Asia, which includes most Arab countries, with over 25,000 non-immigrant visas issued to residents of Saudi Arabia alone.[83] Terrorists are seeking to exploit our immigration systems in order to enter the United States legally, through both the immigrant and non-immigrant visa processes, and possibly illegally, by bypassing official ports of entry along our porous land and sea borders.[84] In any case, a foreigner's contact with a federal or state government employee will almost certainly include name-based identification. While total figures for visa issuance for all foreign countries and both legal and illegal immigration have been discussed thus far, the remainder of this section will focus on Arab-Muslim countries and legal entry specifically.

Name-based identification systems are at the heart of personal identity systems worldwide. Even the most advanced biometric identification systems are ultimately linked to a set of personal identification information that includes a name. As such, name-based identification systems remain an important aspect of the national security efforts currently undertaken by the United States Government. Unfortunately, the collection and use of this information is disparate at best and regularly relies upon the individual preference of a United States Government employee, specifically his or her training and experience.[85] Translation, collection and screening policies are non-existent or highly inept. For example, U.S. immigration law allows for self translation of supporting

---

[82] U.S. Department of State, *Immigrant and Non-Immigrant Visas Issued at Foreign Service Posts Fiscal Years 2002-2006*, http://www.travel.state.gov/xls/FY06AnnualReport.xls (accessed November 18, 2007).

[83] Ibid.; In addition, it is estimated that over 1.3 million people entered the United States illegally in the years 2004 to 2005 and that the 2006 population of illegal persons in the United States exceeds 11.5 million.

[84] See: Terrorist Travel Report; and Coming to America: Arab Terrorists Crossing Border, Middle Eastern Illegals Find Easy Entrance into U.S. from Mexico, by J. Zane Walley, http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=24987 (accessed December 10, 2007).

[85] Senior State Department Official, interview with author, September 1, 2007.

documents.[86] Virtually all current collection practices are based upon U.S. naming conventions that do not take into account the natural genealogical information inherent in Arab-Muslim names.[87] Archaic record keeping systems and paper-based records may have made these issues seem insurmountable in years past. The sheer number of persons entering the U.S. legally each year, the relative distance between foreign consulates and U.S. ports of entry, and the federal disconnect between the Department of State and Immigration and Customs Enforcement (formerly Immigration and Naturalization Services and U.S. Customs) made these tasks impossible. Attempts at stopping terrorism, specifically denying entry of suspected terrorists, routinely relied upon these old fashioned tools prior to 9/11. However, at the dawn of the 21st century, we have a powerful new weapon that has not been properly implemented to combat this issue--technology.[88] As Shane Ham and Robert Atkinson have noted, "If we had advanced IT tools in place prior to September 11, it is almost certain that some of the terrorists would have been detained, and possibly some of the plots would have been foiled."[89] In their policy brief, Ham and Atkinson reference the ability of technology to improve data sharing and bolster identity management efforts.[90] This is not to say that all technological systems prior to 9/11 were incapable of interdicting terrorists, but, as the 9/11 Commission pointed out their use was likely sporadic and disconnected among the many federal agencies responsible for such interdiction. When considering the tools that were in place prior to 9/11 and those that have been implemented after the fact, all fall short of comprehensively addressing the issues outlined here and are arguably based upon ineffective policy and system design and implementation.

As with most reactive policy decisions, many post 9/11 border security strategies, including name-based identification system issues, have been lost in the acceleration of

---

[86] Edwin T. Gania, *U.S. Immigration Step by Step*, 3rd Edition (Naperville: Sphinx, 2006), 142, 305.

[87] Ibid., Appendix E, 243-305.

[88] Progressive Policy Institute, *Using Technology to Detect and Prevent Terrorism*, by Shane Ham and Robert D. Atkinson (Washington, DC, Progressive Policy Institute, 2002), 13.

[89] Progressive Policy Institute, *Using Technology to Detect and Prevent Terrorism*.

[90] Ibid.

programs that were designed prior to 9/11.[91] Many new innovative ideas have been cast aside in the rush for a quick fix.[92] This is evident by federal agency reaction to Homeland Security Presidential Directive 2 (HSPD-2), issued in 2001. HSPD-2 was aimed at changing immigration policies by creating an enhanced capacity to deny, detain, prosecute and deport aliens associated with or suspected of being engaged in terrorist activity.[93] In reaction to this call for prevention, most federal agencies responded by accelerating their stateside efforts associated with these mandates.[94] This is simply a mistake by policy makers. By internalizing issues related to border security, policy makers have taken away the natural identification elements found in Arab-Muslim names. Naturally occurring cultural phenomena have been discarded. The genealogical structure of Arab-Muslim names and the fact that terrorists have a high degree of family connectedness has been ignored in order to focus on strategies at home. The 9/11 Commission faulted U.S. leaders for just such narrow mindedness and failure of imagination.[95] What is sorely needed is a commitment to "forward deployment" type policies within immigration and border security initiatives. The use of such policies takes the fight to the enemy on their own turf as far from the United States as possible and uses the enemies own practices, which are overly reliant on family members, against them. Such policies use assets and influence as core tactics to deter opponents from taking aggressive actions and the quick interruption of such actions should they choose to take them anyway.[96]

In addition to the contextual references discussed above, Homeland Security Presidential Directive 11 (HSPD-11), issued in 2004, specifically calls for forward

---

[91] Robert Bach, *Transforming Border Security: Prevention First* (unpublished work, Naval Postgraduate School, Monterey, CA, October 2007), 2.

[92] Ibid.

[93] Ibid., 3.

[94] Ibid.

[95] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, 407, as applied by Robert Bach in *Transforming Border Security: Prevention First* (unpublished work, Naval Postgraduate School, Monterey, CA, October 2007), 2.

[96] Bach, "Transforming Border Security: Prevention First," 1.

deployed identity management strategies in immigration and border security policy when it states that "the policy of the United States will be to enhance terrorist related screening by implementing coordinated and comprehensive approaches to terrorist related screening at home and abroad to include credentialing."[97] HSPD-11 built upon Homeland Security Presidential Directive 6 (HSPD-6), which established the Terrorist Screening Center (TSC). The TSC depends on accurate, name-based, personal identification information to populate the center's database. Consistent transliteration and comprehensive collection of Arab-Muslim names would certainly be viewed as an open minded and imaginative way to properly populate the TSC consolidated terrorist screening database. Not only is consistent transliteration and comprehensive collection an open minded and imaginative concept, it is one that is vital to the name-based identity management systems used to combat terrorism across the globe.

Les Strickland calls for a "fundamental reengineering of the immigration system" to combat issues such as this.[98] Strickland's basic concept is that an individual should prove their merit for entering the United States prior to being granted the right to enter. It is inconceivable to think that a full investigation into the merits of each individual's application could be completed based on the millions of visitors issued visas each year. However, recent technological advances related to link analysis, decision support systems and increasing knowledge flow could provide key decision making information to government officials if initial name-based identification can be properly established. A recent conversation with a senior consular official at a U.S. embassy in a large Arab country revealed that the name-based identification generated by the issuance of a United States Visa is based upon documents provided by the applicant and the consular officials' training and experience.[99] According to this source, there is no document, policy or official procedure related to the spelling or structure of an individual's name when it is entered into the Consolidated Consular Database. In addition, Strickland points out that the Consolidated Consular Database does not interface with any other identification

[97] Weekly Compilation of Presidential Documents, *Homeland Security Presidential Directive 11*, by The Administration of George W. Bush, http://www.gpoaccess.gov, (accessed November 18, 2007).

[98] Ibid.

[99] Senior United States Consular Official, email interview with author, October 30, 2007.

system, but limited data is being shared with Immigration and Customs Enforcement for pilot projects to allow inspectors to verify that the holder of a visa at a point of entry is the same person that applied for the visa.[100] This information, correct or incorrect, is entered into the system based upon the documents filled out and/or submitted by the applicant. It is clearly evident that U.S. Embassies and the Consular Officials that work within them are our most important "forward deployed" asset in the immigration and border security environment. By collecting information and issuing visas based on standardized technological processes, the potential for entrance of nefarious subjects could be greatly diminished.

## E. RENDERING ARAB-MUSLIM NAMES IN ENGLISH

The process of properly rendering foreign language words, including personal names, in an English equivalent has been at the heart of contentious debate for many years. In 1935 T.E. Lawrence noted, "Arabic names won't go into English, exactly….there are some scientific systems of transliteration, helpful to people who know enough about Arabic not to need helping."[101] Hans Wellisch, a well-known scholar in the field stated, "Conversion of scripts is by no means merely a technical operation, nor is it a simple process of substituting the letters of script A for the corresponding letters of script B."[102] The modern synonymous terms for script conversion, transcription and transliteration, are becoming increasingly automated processes and, therefore, add additional complexity to the issue.[103] The study of applied linguistics; in particular, translation by way of natural language processing, has provided a large number of academic variations on the best and most accurate way to technologically render an Arabic name in English. The debate centers on the processes of translation, transliteration, transcription and Romanization. Each of these processes is distinct, but all

---

[100] Lee S. Strickland and Jennifer Willard, "Re-Engineering the Immigration System: A Case for Data Mining and Information Assurance to Enhance Homeland Security," *Bulletin of the American Society for Information Science and Technology*, vol. 29, no. 1, October/November 2002, 24.

[101] T. E. Lawrence, *Seven Pillars of Wisdom* (New York, NY: Anchor, 1991), 672.

[102] Hans W. Wellisch, *The Conversion of Scripts: Its Nature, History and Utilization* (New York, NY: Wiley, 1978), 509.

[103] Wellisch, *The Conversion of Scripts*, 2.

attempt to provide the same information, an accurate English version of an Arabic name. Translation is the linguistic base of all of the concepts and centers on the interpretation of script or spoken word in one language and the production of script or spoken word in another language that communicates the same message.[104]

> ***Romanization*** is the representation of a language written in a non-Roman script using the Roman alphabet. This includes both transliteration and transcription, e.g. محمد is transliterated as \mHmd\ and transcribed as *Mohammed, Muhammad*, or *Mohamad*, among many others.
>
> ***Transliteration*** is a representation of the script of a source language by using the characters of another script. Ideally, it unambiguously represents the graphemes, rather than the phonemes, of the source language. For example, محمد is transliterated as \mHmd\, in which each Arabic letter is unambiguously represented by one Roman letter, enabling round-trip conversion.
>
> ***Transcription*** is a representation of the source script of a language in the target script in a manner that reflects the pronunciation of the original, often ignoring graphemic correspondence.[105]

Most previous academic works attempt to address only one of these processes, and all seem to have their own drawbacks. This study will not be able to fully discuss the different models for accurate translation, transcription, transliteration or Romanization of Arabic to English in this forum. However, I have chosen several academic attempts that sought to solve the most poignant issues to discuss further.

A large body of academic literature seeks to describe the use of diacritics in Arabic as a methodology for creating an English version of an Arabic name. Merriam Webster On-line defines diacritics, also known as diacritic marks, as marks near or through an orthographic or phonetic character or combination of characters indicating a phonetic value different from that given the unmarked or otherwise marked element.[106] Diacritic marks in written Arabic take the place of some consonants and most vowels normally found in written English. It is the lack of use of diacritics in written Arabic

---

[104] Wikipedia, "Translation," *St. Petersburg: Wikipedia Foundation*, http://en.wikipedia.org/wiki/Translation (accessed October 7, 2007).

[105] Jack Halpern, *Automatic Romanizer of Arabic Names – ARAN*, (Tohoku: CJK Dictionary Institute, 2006), http://www.kanji.org/cjk/arabic/aran/htm (accessed August 10, 2007).

[106] Merriam-Webster Online, *Diacritic*, http://www.m-w.com/dictionary/diacritic (accessed September 11, 2007).

names that is most problematic in the Arabic to English process. Using diacritics results in a vocalized version of a name, while failing to use diacritics results in an un-vocalized version. Un-vocalized Arabic allows for a wide range of options for human and machine translators. Human translators and linguist developed algorithms used in machine translation base their translations on training, experience and personal preference, all of which are variable and result in a wide variety of spellings for the same name. The result has been a large number of technology-based natural language processing solutions that convert information from computer databases into normal sounding human language, each proposing to be the most accurate and dependable solution for Arabic to English translation.

In concert with this approach, Slaliba and Dannan attempted to account for the lack of diacritic marks in written Arabic names when they proposed a morphological approach for automatic diacritic generation in 1989.[107] Morphological approaches to written language are concerned with the structure of words, rather than the single characters within them. The authors were concerned with the structure and complexity of Arabic words and with a technological solution that would add diacritic marks in written Arabic names allowing them to be transliterated easier and more consistently.[108]

Building upon the work of Slaliba and Dannan, the Automatic Understander of Arabic (AUA) was proposed by Nabil Ali in 1992.[109] Ali explains his system as follows:

> The author had to develop a morphological processor capable of analyzing any Arabic word into its morphological primitives, as well as synthesizing the final form of words out of these primitives. Lastly came the syntactical level, which no doubt proved to be the most difficult, primarily because Arabic is usually written without vowels. In essence, written Arabic is a quasi-stenographic script, and this results in a severe mélange of various ambiguities, which are unprecedented and absent from any other languages. The morphological ambiguity, due to the absence of vowels, is intermixed with other types of ambiguities, mainly those associated with

---

[107] B. Slaliba and A. Al Dannan, "An Approach to Automatic Vowelization of Arabic Texts," *paper presented at the 2nd Conference on Arabic Computation Linguistics*, Kuwait, 1992.

[108] Slaliba and Dannan, "An Approach to Automatic Vowelization of Arabic Texts."

[109] Nabil Ali, "Parsing and Automatic Diacritization of Arabic: A Breakthrough," *paper presented at the 13th National Computer Conference*, Riyadh, 1992.

> word sense, parts of speech, and syntactical structure. For a non-Arabic speaker to appreciate such a problem, let us assume hypothetically that an English sentence such as "SOME FIRMS LEND MONEY" is written in the Arabic fashion. The result will be the following string of consonants: "SM FRMS LND MNY" Each of these consonantal forms may have a set of alternative vowelized interpretations.[110]

Evolving from these earlier works, Al Anzi proposed his Stochastic Envelope Model in 2004.[111] A stochastic model is one that lies heavily upon probability, making it highly mathematical in nature.[112] Al Anzi made use of n-grams, otherwise known as letter sequences, to predict the letters within a name and accurately transliterate the name. His model required the creation of a core database of names with proper diacritic marks, a corpus database of grams and patterns by name segmentation, the computation of frequencies of the different grams and patterns from the corpus database and, finally, the development of a stochastic model for how probable a consequent gram or pattern will occur in any position of a name.[113] Al Anzi then enhanced his stochastic model by producing what he terms an envelope core database that is based on name patterns, rather than names themselves.[114]

High error rates and the inability to process a large percentage of names by less error prone solutions have plagued most of the technological solutions developed so far.[115] However, there is one researcher that seems to attempt to address these issues. Jack Halpern at the CJK Dictionary Institute in Japan is currently developing a Natural Language Processing system named the Automatic Romanizer of Arabic Names (ARAN).[116] Halpern's proposed technological solution relies on an eight component process that attempts to account for all of the pitfalls associated with the accurate

---

[110] Ali, "Parsing and Automatic Diacritization of Arabic."

[111] Fawaz S. Al-Anzi, "Stochastic Models for Automatic Diacritics Generation of Arabic Names," *Computers and the Humanities*, 38, no. 4 (2004): 469-481.

[112] Ibid.

[113] Ibid.

[114] Ibid.

[115] Halpern, *Automatic Romanizer of Arabic Names*.

[116] Ibid.

Romanization, transcription, translation and transliteration of Arabic names to English. [117] Halpern goes beyond earlier research and solutions by combining several schools of thought on the best way to complete the Arabic to English process. He uses a comparative approach to establish the "best transliteration possible" by considering phonemic (how words sound when spoken), graphemic (consideration of the sets of letters that make up sounds), phonetic (representation of speech sounds by special characters) and popular (transliteration of names by comparing to the most common spelling of a name). See Table 2, which is listed below, for an explanation of outputs from the various ARAN modules.[118]

| **Unvocalized** | **Vocalized** | **Phonemic** | **Graphemic** | **Phonetic** | **Popular** |
|---|---|---|---|---|---|
| (input) | (ADAN) | (ATAN) | (AXAN) | (APAN) | (AVAN)* |
| محمد | مُحَمَّد | muHammad | mHmd | muħɛ̈ mmɛ̈ d | Muhammad |
| قـــابوس | قَابُوس | Qaabuus | qAbws | qɑ: bu: s | Qaboos |
| جمال | جَمَال | Jamaal | jmAl | dʒɛ̈ mɛ̈ : l | Jamal |
| مكة | مَكَّة | Makka | Mkp | Mɛ̈ kkɛ | Mecca |

*Only one popular variant is shown, but in reality there could be dozens. For example, for قابوس AVAN generates *Qabuus, Qabus, Qabous, Qabooss,* … and many more.

Table 2. Output from Various ARAN Modules

It appears that academic linguists are concerned with producing the "most correct" version of name in the Arabic to English process, which may not be the smartest practice when considering the operational concerns of homeland security. As is the case with most academicians, each can provide logical and defensible reasons for their version of the Arabic to English process. What is most important for America's homeland security is accuracy and consistency in this process. The Arabic language and the academic processes that render Arabic names in English are highly complex. Therefore, they do not lend themselves to an easy solution. However, a consistent, fool-proof and logical system is needed to safeguard the United States against the egress of persons that wish to enter the United States to do harm to her citizens.

[117] Halpern, *Automatic Romanizer of Arabic Names*.

[118] Ibid.

The competing academic schools of thought regarding the proper rendition of Arabic names in English has led to large-scale inconsistency between manufacturers of the technological solutions that have been developed for this process. There are many commercial technological solutions that attempt to solve the issue of accurately and consistently rendering names from Arabic to English. Language Analysis Systems, recently acquired by IBM, was the pioneering corporation in the field.[119] However, two current solutions seem to be frontrunners among all others in this area; Basis Technologies' Transliteration Assistant and Harbinger Technologies' Foxhound.

Basis' Transliteration Assistant is available as a plug-in productivity enhancer software solution for use with Microsoft applications or as a web-based transliteration solution.[120] The user inputs an approximate English spelling of an Arab-Muslim name and the system provides a list of variant spellings.[121] The user must then choose the correct Arabic spelling of the name and then the solution provides the correct English spelling according to Intelligence Community Standards or other widely used U.S. Government Standards as designated by the user (See Figure 2 – Basis Transliteration Assistant).[122]

[119] Richard Lutz, telephone interview with author, July 9, 2008.

[120] Basis Technology, *Transliteration Assistant*, http://www.basistech.com/transliteration-assistant/ (accessed June 1, 2007).

[121] Ibid.

[122] Ibid.


Figure 2. Basis Transliteration Assistant

Additional transliteration standards available within the Basis System include Buckwalter, Board of Geographic Names, Foreign Broadcast Information Service, Standard Arabic Technical Transliteration System and Basis' own proprietary transliteration system.[123] None of these standards were explained in further detail, but all are internationally recognized standards except for their own model. Based upon limited information provided on the company's website, the software uses a database lookup mechanism to match similar names to the IC standard version (possibly an n-gram stochastic model or topological model).[124] If the name cannot be found in the database, it is transliterated in an unknown fashion based upon the IC standard.[125] Further information about specific concepts used by Basis to complete transliterations could not be found on the company's website or elsewhere. Attempts to contact the company for further information and an evaluation of their product via email and telephone were also

[123] Quamus, Tim Buckwalter, *Transliteration*, http://www.qamus.org/transliteration.htm (accessed September 25, 2007); United States Board of Geographic Names, *BGN Home*, http://geonames.usgs.gov/ (accessed October 7, 2007); Note: There was no source located for this system of transliteration. FBIS was transferred to the Director of National Intelligence and renamed the Open Source Center in 2005; Languages of the World, *SATTS*, http://www.languages-of-the-world.us/YourNameIn/SATTS.html (accessed October 7, 2007).

[124] Basis Technology, *Transliteration Assistant*.

[125] Ibid.

unsuccessful. It is assumed that the company does not wish to release this information for proprietary reasons. Extensive research regarding the Intelligence Community Standard found little information. However, the basic information received through a third party appears to provide a fairly consistent transliteration mechanism.[126] Like similar systems, the IC Standard System allows for the use of alternative vowels for some Arabic characters. This perpetuates multiple spelling combinations for the same Arabic name. According to Richard Lutz, additional information about the IC Standard for Arabic transliteration is currently classified or otherwise protected as information that is "For Official Use Only" and, therefore, it will not be included in this study.[127] At face value, the software appears to be a good tool for persons with moderate knowledge of Arabic and enjoys the support of the knowledge management community as the industry leader.[128] This support aside, Basis recognizes that "there is no one 'right' transliteration."[129] Academically, this may be true, but in an operational context it is much more important to be consistent when considering the security of the U.S. homeland. The fact that a user must choose the correct Arabic spelling of a name prior to receiving an English equivalent would make it difficult for most non-linguist U.S. government employees to use.

Harbinger's Foxhound attempts to provide a correct name transliteration and a genealogical link analysis tool.[130] According to the Harbinger Technologies' website, "Foxhound is designed to remedy the transliteration and link-analysis problem inherent to counterterrorism investigations."[131] Their technology combines mathematics, computer science and linguistics, assigning tokens to word parts and then searching phonetically using the principles of mathematical topology to create name variant matches (See Figure

---

[126] Richard Lutz, telephone interview with author.

[127] Ibid.

[128] Greg Pepus, KM World, *Speaking in Tongues: Foreign language KM Technologies*, (July 10, 2007), http://www.kmworld.com/Articles/PrintArticle.aspx?ArticleID=36893 (accessed September 30, 2007).

[129] Basis Technology, *Transliteration Assistant*.

[130] Harbinger Technologies Group, *Foxhound*, http://www.harbingertechnologiesgroup.com/technical-solutions/foxhound.html (accessed August 1, 2007).

[131] Ibid.

3 – Harbinger Foxhound).[132] Mathematical topology concerns itself with higher dimension geometry, specifically connectedness, compactness and continuity. At its most basic level, topology explains that the external appearance of a given shape may take many forms, but the structural base can remain the same and is, in fact, the same as long as no cutting or gluing is involved.[133] It is, therefore, assumed that Harbinger uses this theory to explain connectedness between two or more names, even though they can be spelled many different ways in English.

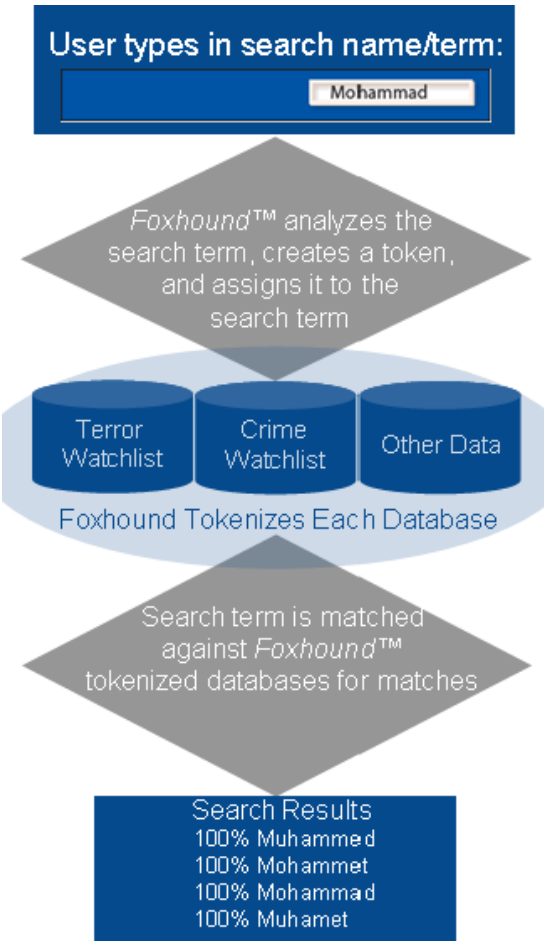


Figure 3. Harbinger Foxhound

[132] Harbinger Technologies Group, *Foxhound*.

[133] Robert Bruner, Wayne State University, *What is Topology*, http://www.math.wayne.edu/~rrb/topology.html (accessed September 25, 2007); Neil Strickland, University of Sheffield Staff, *What is Topology?*, http://neil-strickland.staff.shef.ac.uk/Wurble.html (accessed September 25, 2007).

By assigning a token to each of the topologically identical names listed at the bottom of Figure 3 above, the Foxhound system allows for a 100% match of names that are composed of dissimilarly structured letters.[134] Foxhound seems to be more concerned with matching variant spellings of the same name than providing a correct and consistent transliteration. In fact, Harbinger's website and resources are less revealing than Basis Technologies. No information was found regarding how the system actually transliterates a name or how it performs a link analysis. As with Basis, requests for more information or access to their system for academic evaluation purposes were ignored. Without a broader base of information to complete a full evaluation, it must be concluded that the Foxhound system is a much less viable solution than the Basis system.

The National Geospatial Intelligence Agency (NGA) and the National Security Agency (NSA) have both been working on their own versions of transliteration and name recognition software. The NSA program is called "Aladdin Name Matcher" and is focused on the use of fuzzy name matching technology.[135] The NGA program is called "NGA GEOnet Names Server" and focuses on providing a multiple level transliteration and name matching tool for over 70 different transliteration styles.[136] Neither of these programs is designed to provide a single, standards-based transliteration for use in the personal identity sector. Rather, they are designed to work with a variety of intelligence issues that are largely related to name matching and not name generation.[137]

It is apparent from the review of academic literature, government projects and commercially available solutions that a correct and consistent process for rendering Arabic names in English remains elusive. What is less apparent is whether or not a system already exists or is in the process of being developed. More apparent is that the focus of research and development in this area has been on finding ways to match variant

---

[134] Harbinger Technologies, *Foxhound*.

[135] "Aladdin Name Matcher – Name Matching by Nomalization of Both Query and Data," *National Security Agency Central Security Service*, http://www.nsa.gov/techtrans/techt00066.cfm (accessed August 1, 2008).

[136] "NGA GEOnet Names Server," *National Geospatial Intelligence Agency*, http://earth-info.nga.mil/gns/html/index.html (accessed August 1, 2008).

[137] Peter Viechnicki, email interview with author, July 9, 2008; Richard Lutz, telephone interview with author.

transliterations and spellings of topologically identical names. In any case, there is little indication that academia or private industry are concerned with the combination of variables such as name structure, genealogy or consistent identification through collection of additional, non-biometric, personal identification information. Richard Lutz, a nationally recognized natural language processing expert, agreed that it is feasible to develop an operational level computer solution that consistently renders Arabic names in English.[138] However, Lutz warned that forensic information about the native spelling of an individual's name must be maintained to preserve the ability of intelligence analysts and academic researchers to fully explore the location of origination and validate an individual's personal, name-based identity.

## F. THE STUDY OF KNOWLEDGE, KNOWLEDGE DYNAMICS, AND KNOWLEDGE FLOW THEORY

What is ultimately sought from this project is knowledge; knowledge that will prevent terror attacks upon the United States. This research project began with the assumption that the knowledge needed to meet this overarching goal is either already present or obtainable. While not understood at the beginning of this project, a review of the literature has revealed that Knowledge Flow Theory must be explored to gain an understanding of why such stagnant or obtainable knowledge has not been previously realized or leveraged.

Epistemology, the study or theory of the nature and grounds of knowledge, has it roots in the works of the great Greek Philosophers. Both Plato and Aristotle saw knowledge as something that was absolute and permanent.[139] Over time, the study of knowledge has changed from this early concept through an evolutionary cycle that has led to the contention that knowledge is adaptive and active.[140] To understand Knowledge Flow Theory, one must not only understand this history of epistemology and accept that

---

[138] Richard Lutz, telephone interview with author.

[139] "Epistemology Introduction," *Principa Cybernetica Web*, http://pespmc1.vub.ac.be/EPISTEMI.html (accessed February 3, 2008).

[140] Mark E. Nissen, *Harnessing Knowledge Dynamics: Principled Organizational Knowing and Learning* (Hershey: IRM Press, 2006), vi.

knowledge is both active and adaptive, but must also embrace the concept that knowledge exhibits physical properties such as inertia. More importantly, it exhibits the physical tendency to stay at rest unless placed into motion.[141] Knowledge is distributed unevenly; it moves, clumps and, most importantly, accumulates within specific people and organizations and at specific locations and times.[142]

The lexica of the various disciplines found within the field of Homeland Security do not readily include the concepts of "knowledge dynamics," or "knowledge flow theory." These concepts are fairly new to homeland security and have previously been the focus of academics in the field of Business Management and, more recently, those working with the U.S. military.[143] Understanding the basic concept that knowledge is distinct from information and data, in that it actually enables action, is an important factor for the success of current and future homeland security and counter-terrorism initiatives. For example, the core concept in homeland security since the attacks of September 11, 2001 has been increased information sharing. However, an increase in information still does not allow homeland security professionals to "connect the dots." There was a lot of "information" available about the 9/11 Hijackers before they attacked, but there was little knowledge regarding their motives, intent, personal identities or familial connections that could have aided in preventing the attacks. Homeland security professionals must have, use and leverage knowledge, not just data and information, in order to make decisions that will adequately secure our nation, including its personal identity systems. The advanced concept that knowledge moves and flows from how and where it exists to how and where it is needed is an extremely important notion for those wishing to have the greatest impact on emerging organizational structures, concepts, and systems within the field.[144] It is the clear understanding and application of these concepts that will allow the

---

[141] Nissen, *Harnessing Knowledge Dynamics*, xv.

[142] Mark E. Nissen, "Dynamic Knowledge Patterns to Inform Design: A Field Study of Knowledge Stocks and Flows in an Extreme Organization," *Journal of Management Information Systems* 22, no. 3 (Winter 2005): 225-263.

[143] Ibid.; Hai Zhuge, "Knowledge Flow Network Planning and Simulation," *Decision Support Systems* 42, no. 2 (November 2006), 571-592; Naval Postgraduate School, *Contextual Criticality of Knowledge-Flow Dynamics: The Tragedy of Friendly Fire*, by Mark E. Nissen, Erik Jansen, Carl Jones and Gail Thomas (Monterey, CA: Office of Naval Research, 2003).

[144] Nissen, *Harnessing Knowledge Dynamics*, vi.

United States and its allies to gain and sustain competitive advantage over their adversaries in the Global War on Terror. The lack of knowledge flow, the failure to get knowledge from where it is stagnant to where it needs to be, is the greatest challenge faced by practitioners charged with prosecuting the Global War on Terror. The multi-disciplinary nature of homeland security and counter-terrorism exasperates this issue and limits knowledge flow even further.

The 9/11 Commission stated in its final report that, "we have tried to remember that we write with the benefit and handicap of hindsight…we asked ourselves, before we judged others, whether the insights that seem apparent now would really have been meaningful at the time, given the limits of what people then could reasonably have known or done."[145] By this statement, it is clear that they recognize that knowledge may have prevented the attacks on 9/11, but that people may not have had the knowledge they needed to do so. It was only with the benefit of hindsight that the intelligence community was able to connect the dots. The theory of knowledge dynamics and knowledge flow would argue that by understanding the dynamics of knowledge we can fix the problems related to slow or non-existent flows of knowledge. While the 9/11 Commission may not have understood or been referring to knowledge as it is discussed here, their statement supports the hypothesis that a lack of knowledge flow allowed the greatest industrialized nation in the world to fail at preventing the attacks through knowledge that was already within the system and was well within reach. The Commission recognized ten "Operational Opportunities" that might have foiled the 9/11 attacks.[146] Upon reviewing these ten opportunities, it is clear that all but one is directly related to either a lack of knowledge by one or more federal agencies or the lack of knowledge flow between federal agencies. The Commission uses knowledge related comments to explain each of them, including statements such as, "…FBI headquarters does not recognize the

[145] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, 339.

[146] Ibid., 355-356.

significance of the information…," to describe how the operational failures that led up to 9/11 went undetected throughout the 21 months prior to the successful attacks.[147]

According to Mark Nissen, "the knowledge of how to diagnose and enhance knowledge flows exists today."[148] By employing the principles of this emergent theory, it is expected that academics and practitioners working in a variety of fields can work together to develop ways to avoid the mistakes of the past and discontinue the trial and error practices that have been prevalent since 9/11. This is not to say that there have not been attempts to increase knowledge within homeland security since 9/11. To the contrary, many projects have been initiated in hopes of "connecting the dots" before another terrorist attack occurs. However, the focus of these projects seems to be relegated to information and information sharing. So much so, that now there is too much information to make sense of it all. As such, it appears that knowledge flow has actually slowed instead of increasing as expected. Even those projects that distinguish the concept of "knowledge" as an important factor do not seem to fully distinguish between knowledge and information and certainly do not seem to understand that knowledge is dynamic. To further examine this phenomenon, we will discuss two federally funded homeland security projects in the next two paragraphs. One of them fails to adequately incorporate these concepts and one fully incorporates them. By following the lead of the latter and fully incorporating the idea of knowledge dynamics in the conceptual model described in Chapter III, the U.S. government can realize an overarching system that is designed to mitigate the issuance of ambiguous name-based personal identity documents and identify those that wish to do harm to its citizens.

The Terrorism Liaison Officer (TLO) program developed by Anthony Lukin through the California Commission on Peace Officer Standards and Training is an excellent example of failing to understand knowledge flows. His attempt to "improve the communication, cooperation and coordination between local, state, and federal law enforcement agencies" is counter-productive to producing a sustained increase in

---

[147] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, 355-356.

[148] Nissen, *Harnessing Knowledge Dynamics*, x.

knowledge flow.[149] The program is designed to build a national interconnected program of designated law enforcement officers to attend a course of instruction and fill the specific role of "liaison" for all terrorism related issues handled within their department.[150] By designating a single person within a policing agency that is the "person with the answers to questions concerning terrorism," Lukin's concept stifles knowledge flow. It does so by creating a "knowledge clump."[151] A knowledge clump is defined by Nissen as "knowledge that collects at some isolated coordinate" and is symptomatic of flow pathology to be found within an organization where knowledge flow is not being properly addressed.[152] Lukin indirectly recognizes that isolating such vital knowledge in one individual is problematic, because he suggests a strict selection criterion that includes selecting an individual that will stay in the TLO position for at least 2 years.[153] However, by doing so, he may also be advocating for someone to fill a knowledge critical position that is not expected to stay in the position for more than two years and provides no technological solution to fill the gap. This is likely to further exasperate the issue of knowledge flow within those organizations. If the person selected for the TLO position leaves after two years, the knowledge that he gained to do the job and by actually performing the job leaves with him. Knowledge flow, therefore, ceases and the process has to be started again from the beginning. The TLO program is conceptually sound regarding the need to train local and state law enforcement officials in counter-terrorism. However, its concepts lack recognition of the importance of knowledge dynamics and sustained knowledge flow. What homeland security academics and professionals must focus on when developing these types of programs is not just creating knowledge for a short period of time, but creating sustainable knowledge that can be continually leveraged over time to create a competitive advantage for the United

---

[149] U.S. Department of Homeland Security, *The Terrorism Liaison Officer: A National Strategy - A Conceptual Proposal for the Office of Domestic Preparedness*, by Anthony Lukin, Date Unknown, 1.

[150] U.S. Department of Homeland Security, *The Terrorism Liaison Officer*, 1.

[151] Ibid., 2.

[152] Nissen, *Harnessing Knowledge Dynamics*, 251.

[153] U.S. Department of Homeland Security, *The Terrorism Liaison Officer*, 4.

States. The substantive theory and conceptual model proposed in Chapter III are designed to recognize and eliminate these types of knowledge clump and knowledge flow issues.

*Praestantia Per Scientiam* is the motto of the Naval Postgraduate School and is transcribed from Latin to English as "Excellence through Knowledge." The term aptly describes the programs and goal of the school. The DHS sponsored Center for Homeland Defense and Security at NPS is a prime example of an attempt at increasing knowledge flow in the rapidly evolving field of Homeland Security. The Center has taken on educational responsibilities on a variety of fronts, offering a Masters Degree, an Executive Leadership Program, a Mobile Education Team Program, a Certificate Program, an Agency and University Partnership Program and a general On-Line Course Program. The programs are focused on assisting leaders in Homeland Defense and Security in the development of policies, strategies, programs and organizational elements needed to defeat terrorism in the United States.[154] The Center's programs allow leaders to gain the analytic skills and substantive expertise they need to effectively counter modern terrorism.[155] The Center recognizes its role in increasing knowledge flow within its Vision Statement, which states in part:

> The Center will become the nation's leading educational institution for the innovation and refinement of highly relevant curricula, the creation of depositories of applicable knowledge and the national center for the distribution, transfer and exchange of Homeland Defense and Security information and educational products.[156]

The Center's Program Goals also address knowledge flow when they speak of increasing national capacity for Homeland Security by advancing the study of Homeland Security as "a substantive field of research, scholarship and professional discipline" and that they wish to "create a multiplier effect" by sharing content, results and resources to build preparedness through education.[157] At the core of the Center's mission is the

---

[154] "About the Center for Homeland Defense and Security," *Center for Homeland Defense and Security*, https://www.chds.us/?about (accessed February 3, 2008).

[155] Ibid.

[156] Ibid.

[157] Ibid.

University and Agency Partnership Initiative (UAPI). This program, whether by design or default, is specifically aimed at increasing knowledge flow. The Center's website explains the UAPI Program as follows:

> The University and Agency Partnership Initiative, or UAPI, brings together institutions nationwide dedicated to advancing homeland security education. This effort seeks to increase the number and diversity of students receiving homeland security education, accelerate the establishment of high-quality academic programs, and provide opportunities for collaboration that create an intellectual multiplier effect that furthers the study of homeland security. The Naval Postgraduate School Center for Homeland Defense and Security (CHDS) makes available through the partnership its curriculum, distance learning technology, Homeland Security Digital Library, and all other resources. In return, partners share their curriculum and specialized expertise with the UAPI partners. This provides a cost-effective way to educate thousands of students beyond the NPS campus by reducing the time and resources required of universities and agencies having to build their own curricula and programs from scratch. It also brings synergy to addressing critical research issues, accelerates the development of the homeland security academic discipline, and more rapidly serves knowledge to support the nation's security efforts.[158]

This is one of the few DHS sponsored projects aimed directly at increasing knowledge flow in Homeland Security, but it also exhibits the biggest issue in increasing knowledge flow, time poverty. Things that substantially increase knowledge - such as undergraduate coursework, Masters Programs, and Mobile Education Programs - all take a tremendous amount of time. Therefore, increasing knowledge flow in a timely manner is also important. The implementation of an overarching technological framework, such as the one proposed in Chapter III, appears to recognize the principles of knowledge dynamics and knowledge flow theory and appears to provide a viable solution for the time poverty problem by its use of transactional and analytical process systems. These new technological process systems would relieve current time poverty issues encountered by the human actors involved in name-based personal identity processes.

---

[158] "University and Agency Partnership Initiative," *Center for Homeland Defense and Security*, https://www.chds.us/?special/info&pgm=Partner (accessed February 3, 2008).

The overarching goal of studying knowledge flow is to increase the flow of knowledge from where it is to where it needs to be and the speed at which it does so in order to gain a competitive advantage. Merely moving information around by computers, networks, reports or communications does not address the flow of knowledge.[159] It is clear that increasing knowledge flow is a key to success in most any competitive endeavor. Homeland security and counter-terrorism, especially those activities related to personal identity, are just such competitive endeavors and would do well to develop future programs based on the principles found within the study of knowledge dynamics. Focusing program development around these principles and on projects that employ the use of transactional and analytical process systems that bridge the gaps in knowledge inherit to personal identity may lead to the sustained competitive advantage necessary to defeat the current transnational terrorist threat.

## G. KNOWLEDGE MANAGEMENT

Once a large amount of new knowledge is gained, managing it becomes a monumental task. Knowing where knowledge lies and how to access it is just as important and sometimes more important than gathering it in the first place. In order to effectively mitigate the issuance of ambiguous name-based personal identity documents, it will be highly important to manage the knowledge we obtain about individuals so that all the transactional and analytical processes described in Chapter III can occur seamlessly. As evidenced by its successful impact on business, effective Knowledge Management (KM) has the potential to provide competitive advantage in the Global War on Terror. KM is the systems and processes used to increase knowledge stores and to increase flows between and among the users of the system as discussed in the previous section. It is a concept that revolves around the processes of gathering information and data; organizing it; refining it by discovering relationships, abstracting, synthesizing, and sharing; and disseminating it to people who can use it.[160] Whereas legacy computer systems generally store information and data, knowledge management systems provide a

[159] Nissen, *Harnessing Knowledge Dynamics*, 204.

[160] Housel and Bell, *Measuring and Managing Knowledge*, 12.

way to mirror the human mind's processes of sorting and prioritizing ideas and images.[161] Since 9/11, we have become adept at collecting vast amounts of information and data, but have failed to consistently find efficient ways to share and leverage it. As Thomas Housel and Albert Bell point out, "The central intellectual work of the 21st century may lay not so much in accumulating externalized banks of knowledge as in developing time efficient ways to process selected portions of that knowledge."[162] Knowledge worth having--that knowledge which provides competitive advantage--can only be realized through investment and innovation.[163] KM has evolved from mere data warehousing to an integrated strategy to improve organizational competitiveness and has become the focus of strategic resource allocation in many organizations.[164] There is support within the KM community for a re-defined focus on systems that increase the collaborative capacity of organizations.[165] By focusing on the synergies of knowledge-related capabilities, Nielsen provides a more dynamic perspective of KM that incorporates these ideas.[166] The conceptual model proposed in Chapter III relies heavily upon the principles outlined above and is centered on the concept that a lack of knowledge and knowledge sharing, not a lack of data or information, is the underlying problem associated with name-based personal identity.

## H. INTELLIGENCE & SECURITY INFORMATICS AND KNOWLEDGE DISCOVERY FROM DATABASES

The science of Intelligence and Security Informatics (ISI) is one of the many new trends emerging within the field of Homeland Security and provides a solid, research-based, foundation for the process and analytical portions of the conceptual framework

---

[161] Housel and Bell, *Measuring and Managing Knowledge*, 10.

[162] Ibid., 12.

[163] J. P. Liebeskind, "Knowledge, Strategy, and the Theory of the Firm," *Strategic Management Journal* 17, Special Issue: Knowledge and the Firm (1996): 93-107.

[164] L. A Halawi and R. V. McCarthy, "Knowledge Management and the Competitive Strategy of the Firm," *The Learning Organization* 13, no. 4 (2006): 384-397.

[165] B. B. Nielsen, "Strategic Knowledge Management Research: Tracing the Co-Evolution of Strategic Management and Knowledge Management Perspectives," *Competitiveness Review* 15, no. 1 (2005): 1-13.

[166] Nielsen, "Strategic Knowledge Management Research," 1-13.

presented in Chapter III.[167] By implementing ISI principles as a foundation for the conceptual framework, intelligence and knowledge discovery will be enhanced through standards-based information and data collection, processing, analysis, and utilization.[168] This will, in turn, enhance the use of decision support systems (see next section) within the conceptual framework. Based on enhanced knowledge discovery capabilities, governmental officials will be able to make tactical and strategic decisions and allocate appropriate assets and resources to detect, prevent, deter and respond to future attacks.[169] Most important to this study is the application of ISI within the conceptual framework in support of enhanced intelligence capabilities, "smart borders," and counter-terrorism investigations.[170] The reason for using ISI as a foundation and not the framework for the *Dynamic Identity Grid* discussed in Chapter III is discussed by Chen in Chapter 1 of his most recent work. Chen recognizes three challenges to implementation of ISI systems: the nature of terrorism and terrorist acts, the nature of intelligence related data, and the nature of intelligence analysis techniques.[171] The nature of terrorism and terrorist acts is that they occur across governmental and physical boundaries, with irregularity and without warning, making it difficult to combat with limited resources. The nature of intelligence and intelligence related data is that it naturally becomes stove-piped and regularly overloads individuals and technological systems.[172] The nature of intelligence analysis techniques is that they vary greatly among the many governmental units responsible for using them and that the intelligence analysis community lacks clear standards for their development.[173] Chen writes:

> Facing the critical missions of national security and various data and technical challenges, we believe there is a pressing need to develop the science of Intelligence and Security Informatics (ISI), with its main

---

[167] Chen, *Intelligence and Security Informatics for International Security Information Sharing and Data Mining: Integrated Series in Information Systems*, 182.

[168] Ibid., 3.

[169] Ibid.

[170] Ibid., 4-5.

[171] Ibid., 5-7.

[172] Ibid., 6.

[173] Ibid.

> objective being the development of advanced information technologies, systems, algorithms, and databases for national security-related applications, through an integrated technological, organizational, and policy-based approach.[174]

The concepts of *Dynamic Personal Identity* and the *Dynamic Identity Grid* proposed in Chapter III are expected to meet Chen's objectives from a policy and integrated macro-systems level.

## I. DECISION SUPPORT SYSTEMS

Decision support systems are technological systems that orient themselves based on unfolding circumstances and through gathering of additional knowledge and information.[175] Based on Boyd's "OODA Loop," these systems can be explained as systems that observe, orient, decide and act.[176] "By definition, the purpose of decision support systems is to improve the quality of decisions."[177] These systems compliment human resources that work at a much slower pace, coupling the intellectual capabilities of the individual with the model processing and data storage and retrieval capabilities of the computer to improve the quality of decisions.[178] They also push decision making power to the edge of organizations and across organizational boundaries when allowed to observe and orient themselves to a variety of knowledge, information and data sources. Technological advances have the potential to transform the U.S. intelligence and counter-terrorism functions from a smart-smart-push approach to a smart-pull approach.[179] Smart-smart-push resides within stove-piped structures that require their owners to be

---

[174] Chen, *Intelligence and Security Informatics for International Security Information Sharing and Data Mining: Integrated Series in Information Systems*, 7.

[175] John Boyd, "OODA Loop - John Boyd," Value Based Management, http://valubasedmanagement.net/methods_boyd_ooda_loop.html (accessed June 1, 2008).

[176] Ibid.

[177] David M. Steiger and Natalie M. Steiger, "Decision Support as Knowledge Creation: An Information Systems Design Theory," *Proceedings of the 40th Annual Hawaii International Conference on Systems Sciences* (2007), Abstract.

[178] Steiger and Steiger, "Decision Support as Knowledge Creation: An Information Systems Design Theory," Abstract.

[179] David S. Alberts and Richard E. Hayes, *Power to the Edge: Command and Control in the Information Age* (Washington, DC: Department of Defense, 2003), 259.

smart about knowing what information is important and to whom and also smart about how to push information to those that need it within the timeframe that it is needed.[180] This likely aided in the massive intelligence failures leading up to the 9/11 attacks. However, the advent of robust networks and the internet provides the foundation needed for a smart-pull system where decision support mechanisms within the system eliminate the need for information owners to be smart about who needs their information and what they need.[181] In this sense, the *Dynamic Identity Grid* proposed in Chapter III becomes an "Edge System." An "Edge System" is a system that resides at the edges of the organizations that it serves and empowers the information and knowledge it holds to be leveraged by any number of component systems or individuals that access it.[182] The proposition that a single governmental organization can control all of the components necessary to appropriately leverage knowledge about terrorists and their identities is a mistake. The only way to ensure that knowledge and information are shared and that individuals and organizations will work together to combat the entrance of terrorists to this country is to move power to the edge of the organizations responsible for doing so.[183] When power to the edge theory is fully applied to a system's architecture, the result is an edge info-structure that can inform and assist decisions that must be made on the fly; bringing all knowledge, information and assets to bear on the situation at hand, making the system optimally effective.[184]

## J. BIOMETRICS

Merriam-Webster Online defines "biometrics" as the measurement and analysis of unique physical or behavioral characteristics, especially as a means of verifying personal identity.[185] This is a newer use of the term that is not related to the historical

---

[180] Alberts and Hayes, *Power to the Edge*, xiv.

[181] Ibid., xv.

[182] Ibid.

[183] Ibid., 179.

[184] Ibid., 179-180.

[185] Merriam-Webster, "Biometrics," Merriam-Webster Online Dictionary, http://www.merriam-webster.com/dictionary/biometrics (accessed July 11, 2008).

implications defined by the International Biometric Society as: "the field of development of statistical and mathematical methods applicable to data analysis problems in the biological sciences."[186] For this study, we will use the term as defined by Merriam-Webster Online. According to the Biometric Consortium, "biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic. Biometric features that can be measured include: facial, fingerprint, hand geometry, handwriting, iris, retina, vein, and voice. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions."[187] The fact that the U.S. Government has established a host of groups to work on the issue of biometrics to secure personal identity systems indicates that they are welcomed and needed technologies in the personal identification process.[188] Currently, biometric technologies have been deployed in the FBI's IAFIS Program, the US-VISIT Program, The Transportation Workers Identification Credentials Program, and the Registered Traveler Program.[189] However, the use of biometric technologies is not new to the private sector, many of which use the technologies to secure their property and properly identify their customers and workers.[190] The most well known use of biometrics in the private sector is found at the Walt Disney World Corporation, where they use biometric scanners to ensure the integrity of their customer ticketing system.[191] The National Science & Technology Council's Biometric Identification and Identity Management Subcommittee has made the following statement about the use of biometrics within the U.S. Government:

---

[186] The International Biometric Society, "Definition of Biometrics," *The International Biometric Society*, http://www.biometrics.tibs.org/ (accessed July 11, 2008).

[187] Biometric Consortium, "Introduction to Biometrics," *Biometric Consortium*, http://www.biometrics.org/intro.htm (accessed July 11, 2008).

[188] See Also: Biometrics, Department of the Army, Biometrics Task Force, Executive Agents for Biometrics, http://www.biometrics.dod.mil/ (accessed July 11, 2008); Biometics Catalog, http://www.biometricscatalog.org/Introduction/default.aspx (accessed July 11, 2008); and Biometrics.gov, http://biometrics.gov/ (accessed July 11, 2008).

[189] National Science and Technology Council, "Biometrics Frequently Asked Questions," http://www.biometricscatalog.org/biometrics/FAQDec2005.pdf (accessed July 11, 2008).

[190] National Science and Technology Council, "Biometrics Frequently Asked Questions."

[191] Ibid.

> Government and industry have a common challenge in today's global society to provide more robust identity management tools, and identity governance principles on how to deploy these tools intelligently, to meet national and international needs. Biometrics are the most definitive, real-time identity management tools currently available; however, use of the technology thus far has mainly consisted of systems designed to meet narrow objectives. To fully meet large-scale identity governance requirements, the use of biometrics technology must be made more robust, scalable and interoperable. Meeting these needs will require biometrics technology enhancements, adjustments of commercial business practices and system designs, and development of consensus on social, legal, privacy and policy considerations. Collaboration among the biometrics community—government, industry and academia—on these common challenges is essential.[192]

Interoperability of the likely diverse set of biometric systems that will be used in the *Dynamic Identity Grid* proposed in Chapter III will require strict standards to be useful and successful.[193] The NSTC Subcommittee has established an interoperability working group to assess options and develop plans to support biometric data sharing among U.S. Government agencies.[194] The NSTC Subcommittee is concerned with ensuring interagency consensus on standards-related items required to enable the interoperability of various Federal biometric applications, and to guide federal agencies as they develop and implement related biometric programs.[195] Any use of biometric technology within the conceptual framework should comply with the standards developed by the Subcommittee. Biometrics alone are not enough to counter the current terrorism threat and are designed as an identity verification and authentication component in the overall design of the *Dynamic Identity Grid*. In October 2005, Barry Kefauver of the

---

[192] National Science and Technology Council, "The National Biometrics Challenge," *NSTC Subcommittee on Biometrics and Identity Management*, http://biometrics.gov/Documents/biochallengedoc.pdf (accessed July 11, 2008).

[193] National Science and Technology Council, "Policy for Enabling the Development, Adoption and Use of Biometric Standards," *NSTC Subcommittee on Biometrics and Identity Management*, http://www.biometrics.gov/Standards/NSTC_Policy_Bio_Standards.pdf (accessed July 11, 2008).

[194] National Science and Technology Council, "Policy for Enabling the Development, Adoption and Use of Biometric Standards," 3.

[195] Ibid.

International Civil Aviation Organization told delegates at the 2005 Digital Identity Forum in London that "It (biometrics) is nothing but a tool to enhance the human inspection process," providing greater support for this conclusion.[196]

[196] Jane Wakefield, "Doubts over Biometric Passports," *BBC.co.uk*, http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/4381160.stm (accessed November 25, 2007).

# III. THE RESEARCH: GOALS, METHODS, FINDINGS & SOLUTIONS

Homeland Security is a relatively new field of study that, in its current form, emerged from the attacks on New York City and the Pentagon in September 2001. Prior to that, the earliest reference to anything resembling Homeland Security was made in a 1988 report entitled Catastrophic Terrorism: Elements of National Policy.[197] In this report, the authors recognized that the "security of the American homeland" was the responsibility of the U.S. Atlantic Command.[198] The ideas, concepts and theories within this new field of study are, inherently, emergent in nature. Therefore, this research project, like many others in the field, is based on an inductive research approach that seeks to emphasize the development of insights and generalizations.[199] In this case, the insights and generalizations developed are focused on personal identity, specifically the naturally occurring genealogical attributes of Arab-Muslim personal names and their potential for positive impact on U.S. Counter-Terrorism efforts. It is not classically inductive in the sense that observations were focused on specific people. Rather, the inductive approach used was focused on a broad range of subjects: including professionals within the field of study, government, culture, literature, policy, news and other relevant subject matter in an attempt to provide the overarching insights and generalizations needed to develop effective theory for use in policy and practice initiatives. Specifically, the answers obtained through the research are expected to be used to alter both policy and practice within a broad range of homeland security sectors, including, but not limited to, consular affairs, immigration, border enforcement, counter-terrorism investigation and terrorism related intelligence.

---

[197] Ashton B. Carter, John M. Deutch and Phillip D. Zelikow, *Catastrophic Terrorism: Elements of a National Policy*, http://www.ksg.harvard.edu/visions/publication/terrorism.htm (accessed December 4, 2007).

[198] Ibid.

[199] William L. Neuman, *Social Research Methods: Qualitative and Quantitative Approaches* (Boston: Pearson, 2006), 1-592.

This project demanded the use of a primarily qualitative approach. Answers to the research questions of this study were emergent in nature and, therefore, the methods of this study had to accommodate a nonlinear path that led the researcher in a cyclical and iterative pattern.[200] In other words, the researcher had to be led to conclusions and, in many cases, additional questions based on the research. The data collected in this study was both hard and soft qualitative information. That is, it was in the form soft data such as impressions, ideas, thoughts, or text; as well as in the form of hard data such as numbers and statistics.[201]

## A. RESEARCH GOALS

The primary goal of this research effort was to develop baseline substantive theory and a conceptual systems framework for the field of Homeland Security. Research efforts were primarily related to knowledge management, identity management, knowledge flow theory, Arab-Muslim name structure, existing government procedures and policies, and select terrorist attacks/plots. It is anticipated that the development of such baseline theory and a conceptual model will inspire both the author and others to undertake further, more effectual research regarding these and other related emerging issues. It is suggested that such further research should be focused on testing and extending the theory and conceptual framework developed through this thesis. It is a secondary goal that this and subsequent research will lead to changes in how federal policy and future technological solutions are designed. Specifically, it is a personal aim of the author that the research will lead to changes regarding the collection of Arab-Muslim names; changes in federal law and policies regarding the application for and approval and issuance of U.S. travel visas; and the development of integrated technological solutions that lead to highly collaborative intelligence collection, counter-terrorism investigation and immigration enforcement practices.

---

[200] Neuman, *Social Research Methods: Qualitative and Quantitative Approaches*, 152 – 153.

[201] Ibid., 151.

## B. RESEARCH METHODS

Accepted methods of research were employed in this study to provide a rigorous and logical deduction of literature and findings to support valid conclusions in the way of substantive theory and a conceptual model proposed later in this chapter. The study followed the "hour glass notion" that requires the researcher to begin with broad notions that are narrowed to a manageable level for research and provides conclusions that generalize back to further questions.[202] The specific methods used and discussed below were chosen based on their applicability to the mediums of inquiry employed by the researcher.

### 1. Qualitative Research Design

Qualitative research is concerned with the richness and feeling of raw data and seeks to develop insights and generalizations out of the data collected.[203] By the use of qualitative methods, this project attempts to construct meaning from previously uncorrelated issues. While this project started with a highly focused set of research questions, its focus was further refined and sharpened throughout the research process. As such, the researcher remained open to unanticipated information that was revealed throughout the process and was prepared to change directions as new evidence emerged. "All qualitative approaches have two things in common. First, they focus on phenomena that occur in natural settings – that is, in the 'real world.' And second, they involve studying those phenomena in all their complexity."[204] As with many qualitative research projects, this one was not likely to find a single truth and it did not. As expected, it found multiple perspectives, each of which may have equal validity.[205] Therefore, it became the researcher's responsibility to gain further understanding of the subject matter throughout the research process and ask increasingly specific questions in order to effectively move

---

[202] William M. K. Trochim, "Structure of Research," Research Methods Knowledge Base, http://www.socialresearchmethods.net/kb/strucres.php (accessed July 12, 2008).

[203] Neuman, *Social Research Methods: Qualitative and Quantitative Approaches,* 149.

[204] Paul Leedy and Jeanne Ormrod, *Practical Research: Planning and Design,* 8th Edition (New Jersey: Pearson, 2005), 1-319.

[205] Leedy, *Practical Research: Planning and Design,* 135.

towards the ultimate goal of theory building and conceptual modeling. This study did not take the form of just one qualitative research method. Instead, it was a hybrid qualitative study that borrowed concepts from a handful of formal qualitative methods, including grounded theory, content/document analysis, interviewing, triangulation and conceptual modeling. The implementation of a hybrid qualitative method is not an uncommon way to conduct a qualitative study. According to Eisner, qualitative research methods are the least prescriptive.[206] In fact, Leedy suggests that there are "no magic formulas, no cookbook recipes for conducting a qualitative study." He goes on to say, "In a qualitative study, the specific methods that you will use will ultimately be constrained only by the limits of your imagination."[207] The following sections will describe the specific methods employed in this hybrid qualitative study.

### 2. Grounded Theory

A review of two previous research projects by Mark Nissen and Dennis Gioia and others found that both projects relied upon a multi-stage analytical approach that grounded their research.[208] While this study does not take a pure grounded theory approach, it does share some of its overarching characteristics that are worthy of further discussion. Like these projects, the current research relied upon iterative stages that built upon one another to provide the rigor required of a superior qualitative study. First order research, in the form of content analysis of government reports and open source news products and case study, provided basic assumptions for the researcher to explore further. Second order research built upon the assumptions developed in the first order process, using the first order information as a starting point for second order document analysis and interviewing efforts. The second order document analysis and interviewing confirmed the validity of the researcher's first order assumptions and allowed for

---

[206] Elliot W. Eisner, *The Enlightened Eye: Qualitative Inquiry and the Enhancement of Educational Practice* (Upper Saddle River, NJ: Prentice, 1998).

[207] Leedy, *Practical Research: Planning and Design,* 135.

[208] Dennis A. Gioia, James B. Thomas, Shawn M. Clark, and Kumar Chittipeddi. "Symbolism and Strategic Change in Academia: The Dynamics of Sensemaking and Influence," *Organization Science*, 5, no. 3 (1994): 363-383; Nissen, "Dynamic Knowledge Patterns to Inform Design: A Field Study of Knowledge Stocks and Flows in an Extreme Organization."

triangulation around a set of core principles important to the third order processes of theory building and conceptual modeling. Like Nissen's research, this project went a step further than that of Gioia's in that the tertiary stage allowed the analysis to identify themes that had theoretical relevance and, in turn, a direct impact on the proposed substantive theory and design of the conceptual model.[209]

### 3. Content Analysis

This study borrowed the general principles found within the content analysis research method and applied them to a variety of subject matter. Leedy defines content analysis as "a detailed and systematic examination of the contents of a particular body of material for the purpose of identifying patterns, themes or biases."[210] Neuman defines content analysis as "research in which the content of a communication medium is systematically recorded and analyzed."[211] In the context of this project, the content analysis method was used to gather, code and record relevant information from books, news sources, and government reports to provide context and meaning for the study. Content/Document Analysis was also used to support or refute the various claims made throughout the project that focus on the importance of Arab-Muslim name structure to U.S. Homeland Security. Finally, detailed document analysis was used to support the claim that ambiguous identities are prevalent in the U.S. personal identity system and that U.S. Government forms and documents foster the perpetuation of this issue. In order to accomplish these goals, the researcher had to identify bodies of material to be studied, precisely define the characteristics to be examined and then break them down to manageable segments that were analyzed separately.[212] The use of this method resulted in a description of patterns that the data reflect. This data is discussed both in the literature review found in Chapter II and in the research findings listed below. Within the literature review, this method was used to determine if kinship ties existed among

---

[209] Nissen, "Dynamic Knowledge Patterns to Inform Design: A Field Study of Knowledge Stocks and Flows in an Extreme Organization," 237.

[210] Leedy, *Practical Research: Planning and Design*, 142.

[211] *Social Research Methods: Qualitative and Quantitative Approaches*, 44.

[212] Ibid., 142.

individual terrorists within terrorist groups and/or between individual terrorists and persons that supported their activities; to explore the role of transliteration and related technological systems in the name-based identity process; and to explore the role of knowledge management and related technological systems to be used in the conceptual framework described later in this chapter.

### 4. Interviewing

The interview research method was used to fill gaps in the research by confirming or refuting the assumptions made by the researcher in the primary and secondary phases. Experts were consulted individually and in groups when the literature and data did not provide sufficient evidence for conclusion on their own. Some experts remain non-attributable and are described only by their relative position within government service. As most subjects of the interview process were not readily available for face to face contact, much of the interview process was conducted via telephone or electronic mail.

### 5. Triangulation

The post-positivist research method of triangulation was used to understand the data and provide meaning and context for the researcher.[213] It emphasizes the importance of multiple measures and observations, each of which may have its own errors, to gain a greater understanding of the research outcomes.[214] The use of this method allowed for triangulation around a set of core principles important to theory building and conceptual modeling--the key outcomes of the study. Information obtained during the content analysis phase of the study was relied upon heavily throughout this portion of the project.

### 6. Conceptual Modeling

The use of conceptual modeling as a research method was implemented for the purpose of developing a macro-level integrated system of systems architecture designed

---

[213] Neuman, *Social Research Methods*, 150; William M.K. Trochim, "Positivism and Post-Positivism," Research Methods Knowledge Base, http://www.socialresearchmethods.net/kb/positvsm.php (accessed July 12, 2008).

[214] Trochim, "Positivism and Post-Positivism."

to leverage the knowledge within an individual's *Dynamic Personal Identity*, explained later in this chapter. Leo Apostel contends that we use models in research for a variety of reasons all centered on the goals of explaining theory and bridging the gaps between the theoretical and observational levels of research.[215] Apostel further explains modeling as a way for researchers to develop knowledge about new theory from a zero starting point; to explain theory too difficult to yield solutions given present techniques; to connect disparate theories; to achieve theory completeness; to test known theory; or to explain the facts of a theory.[216] Finally, Apostel explains that a model can take the form of an image, perception, drawing, calculi, language or physical system.[217] The macro-level systems architecture developed during this study is modeled in the form of text and computer drawn images. It is designed to provide both a language-based and visual-based explanation of an abstract conceptual systems architecture developed to bridge the gap from the theory of *Dynamic Personal Identity* to the operational structure of the *Dynamic Identity Grid* that is fully explained later in this chapter.

## C. RESEARCH FINDINGS

Research conducted throughout the initial stages of the research process attempted to answer the first two research questions identified in Chapter I. First, the project focused on determining if Arab-Muslim visitors to the United States are entering with ambiguous name-based identities and/or establishing them after entering the United States. Second, the project focused on determining if United States Government practices related to the collection of Arab-Muslim names and the establishment of associated personal identities is ethnocentrically biased. To answer these questions, two extensive document analyses were conducted.

---

[215] Leo Apostel, "Towards the Formal Study of Models in Non-Formal Sciences," in *The Concept and Role of the Model in Mathematics and Natural and Social Sciences*, edited by Hans Fruedenthal (Dordrecht: Reidel, 1961), 1-37.

[216] Apostel, "Towards the Formal Study of Models in Non-Formal Sciences," 2.

[217] Ibid., 4.

### 1. Identity Ambiguity of Arab-Muslim Visitors to the United States

In an attempt to determine if people visiting the United States from Arab countries are entering the United States with ambiguous personal identities or that they are establishing them after entering the United States, a comprehensive content analysis of the Florida Department of Highway Safety and Motor Vehicles - Driver And Vehicle Information Database (DAVID) was conducted. The Florida DAVID system was chosen, because it includes scanned identity documents of those persons that are issued a Florida Driver License or Identification Card and are not U.S. citizens. It is understood that this information may not be indicative of circumstances in the rest of the United States, but was found to be the most comprehensive information available to the researcher. Only records that included a U.S. travel Visa were included in the sampling. Using a confidence level of 95% and a Margin of Error of 10%, a sample size of 96 individuals was expected to be sufficient for purposes of this research project.[218] One hundred total records were actually reviewed, slightly increasing the probability that the conclusions of this research are accurate. Records for individuals from each of the following countries were reviewed: Saudi Arabia, United Arab Emirates, Yemen, Oman, Kuwait, Bahrain, Qatar, Iraq, Lebanon, Syria, Jordan, Egypt, Mauritania, Sudan, Libya, Tunisia, Algeria, and Morocco. Samples were taken in random order, starting with the first record returned in each set and every fifth record after that up to twenty records per country. However, some countries did not have any records in the system. Of the random sample of records reviewed 80% were of males and 20% were of females. The research found that 98% included a given name, 49% included a single genealogically connected name, 24% included a second genealogically connected name, and 91% included a family or tribal name. Of the records reviewed, only 55% included an exact match between the name listed on the Travel Visa and the name listed on the Florida Driver License/Identification Card. Based on this information it is likely that only 24% of the 100 records reviewed

[218] Six Sigma, "Survey Size Calculator," http://www.isixsigma.com/offsite.asp?A=Fr&Url=http://www.surveyguy.com/SGcalc.htm (accessed December 4, 2007). For further information on determining sample size, see also SixSigma, "How to Determine Sample Size, Determining Sample Size," http://www.isixsigma.com/library/content/c000709a.asp (accessed December 4, 2007).

entered the United States with a U.S. Travel Visa that included their full four part Arab-Muslim name. In addition, only 55% of the 24%, or roughly 13%, actually would have that full Arab-Muslim name listed on their Driver License/Identification Card. Based on this information and the fact that over 2.2 million non-immigrant persons entering the United States from Asia in 2006; we could expect that only 528,000 would have their full Arab-Muslim name listed on their U.S. issued Travel Visa and that only 286,000 would have their full Arab-Muslim name listed on their U.S. issued Driver License or Identification Card. This proves that there is substantial ambiguity in the personal identities of Arab-Muslim persons entering the United States and even greater ambiguity if they obtain a Driver License or Identification Card once they have entered the United States. This easily explains why the 9/11 hijackers used over 300 aliases while in the United States, as discussed on Chapter II.

### 2. Ethnocentricity of U.S. Name Collection Practices

To determine if an ethnocentrically-based bias exists in the collection of Arab-Muslim names by U.S. Government agencies, a multi-stage analytical approach was used to ground the research. The three stage process used sought to find those government documents that were most important in the foreigner entrance process, determine if the data collected by the documents appeared to be ethnocentrically biased, and ensure that other informal processes were not used to collect further information. This three tiered approach to grounding the research is reminiscent of studies by Nissen and Gioia.[219] Like Nissen's research, this project went a step further than that of Gioia's in that the tertiary stage allowed the analysis to identify themes that had theoretical relevance and allow the author to close in on the ability to generalize for all U.S. Government documents used in the foreigner entrance process.[220] Due to time limitations, the author chose to limit this analysis to forms used by U.S. Customs and Immigration Enforcement and the U.S.

[219] Nissen, "Dynamic Knowledge Patterns to Inform Design: A Field Study of Knowledge Stocks and Flows in an Extreme Organization," 237.

[220] Ibid.

Department of State. In doing so, the author accepts that the study's finding cannot generalize for all U.S. Government documents. However, the author is comfortable with the results based on the scope of this project.

### 3. Content Analysis

In order to determine which documents were most important in the foreigner entrance process, a series of interviews were conducted with senior officials from U.S. Immigration and Customs Enforcement and the U.S. Department of State. Initially, these officials directed the author to several on-line and print resources, where most immigration and visa related forms could be found. After collecting a list of the documents, further interviews were conducted to determine which documents were of greatest significance in the foreigner entrance process. After selecting a limited number of documents for further review, a document analysis of several active Immigration and Customs Enforcement subject files was completed to ensure that the forms discussed in the second round of interviews were in fact relevant to this study. Similar files from the U.S. Department of State were not available for review. Based on this initial process, the following document analysis was conducted.

#### *a. U.S. Immigration and Customs Enforcement Documents*

A thorough document analysis of fourteen U.S. Immigration and Customs Enforcement documents found that all fourteen failed to adequately collect the full Arab-Muslim name as discussed in Chapter II. The following forms were analyzed for this purpose: G-14, G-325, G-325A, G-325B, G-325C, I-212, I-131, I-193, I-485, I-539, I-601, I-751, I-765 and N-400. In each case, the forms require the user to input their information in U.S. style of "First, Middle, Last." The forms were found to replace the word "Last" with the word "Family" on twelve occasions and used the word "Given" in place of the word "First" on four occasions. Form G-14 asks simply for "Name." The G-325 series, I-751 and I-765 forms ask for "Other Names Used." The exclusive use of the U.S. structure in the collection of name-based identity information via U.S. Immigration and Customs Enforcement forms appears to be ethnocentrically biased.

### *b. U.S. Department of State Documents*

A thorough document analysis of fourteen U.S. Visa documents found that all fourteen failed to adequately collect the full Arab-Muslim name as discussed in Chapter II. The following forms were analyzed for this purpose: DS-117, DS-156, DS-156E, DS-156K, DS-157, DS-158, DS-230 Part 1, DS-230 Part 2, DS-1648, DS-3023, DS-3032, DS-3035, DS-3052, and DSP-122. In each case, the forms require the user to input their information in U.S. style of "First, Middle, Last." In one case, the term "First" is replaced with the term "Given." In six cases, the term "Last" is replaced with the term "Family," and once it is replaced with the term "Surname." Form DS-156 also asks for "other first and middle names used." Form DS-157 also asks for "Clan or Tribe Name," "Full Name" and allows for multiple "First" and "Last" entries. Form DS-158 allows for multiple "First" and "Last" entries. Forms DS-230 Part 1 and Part 2 ask for "Other Names Used" and "Full Name." Form DS-3035 asks for "Other Surname(s)" and "Other Given Name(s)." While these forms attempt to collect more data than the immigration forms discussed above, they still appear to be ethnocentrically biased towards the U.S. naming structure and certainly are not specific enough to adequately diminish name-based identity ambiguity for those wishing to enter the United States.

## D. SOLUTIONS: THEORY, CONCEPT, ISSUES & STRATEGY

### 1. Dynamic Personal Identity – A Substantive Theory

The American Heritage Dictionary defines dynamic as something of or relating to energy or to objects in motion.[221] Based on the findings of this study, we can conclude that the various components of a person's personal identity, when fused together, can become dynamic. The components are not dynamic in the sense that the person's identity "moves," but that by fusing its parts it becomes something that causes knowledge to move. A "dynamic" personal identity is something that can be leveraged against those things that we already know to provide greater understanding of who a person is, who

[221] Bartleby, "Dynamic - The American Heritage Dictionary," http://www.bartleby.com/61/39/D0443900.html (accessed July 12, 2008).

they are related to and what threat they may pose to the United States. It allows us to get beyond letters and numbers stored on documents and in computers and allows us to see who a person is at a much more complex level--such as who they are based on kinship ties and biometrics--without discarding their basic name-based information. By focusing on the components of personal identity that can be enhanced, personal identity can become a dynamic commodity. Future efforts must be focused on ensuring that the U.S. Government collects, produces, stores, and leverages those components of personal identity that make it dynamic. Personal identity information must be collected with an eye toward kinship and not toward what someone prefers to be called or what fits nicely on pre-printed forms. Identification documents must be produced that are consistent and reliable in their structure and form. Information must be stored in a form that is easily understood and searchable. Finally, technological systems must be designed to properly leverage the information that we produce and store and to increase knowledge flow among our governmental agencies (see next section).

In order to do this, we have to design a systematic set of characteristics that should be collected and design standards for transliteration and biometric collection that do not allow room for differences. Consistency in transliteration is a key aspect to ensure consistency in name-based identity. For a full explanation of this issue, refer back to Chapter II. As the focus of this project was on Arab-Muslim personal identification, it is suggested that we should use the standard four part Arab-Muslim name and several additional characteristics to ensure accuracy and non-duplication. Specifically, it is suggested that the base structure of an Arab-Muslim *Dynamic Personal Identity* consist of an individual's personal name-based identifier, biometrics and photograph. The personal name-based identifier should include the person's *Ism* (given name), the 1st *Nasab* (Father's *Ism*), the 2nd *Nasab* (Paternal Grandfather's *Ism*), *Hisba* (Family Name), Date of Birth, City of Birth, Mother's *Ism* (Given Name), Mother's Date of Birth, Mother's City of Birth, Father's Date of Birth and Father's City of Birth. These characteristics can be collected, stored and leveraged in their aggregate form to provide a comprehensive and "dynamic" personal identity for U.S. officials. See Figure 4 below for a depiction of the characteristics of a "Dynamic Personal Identity."

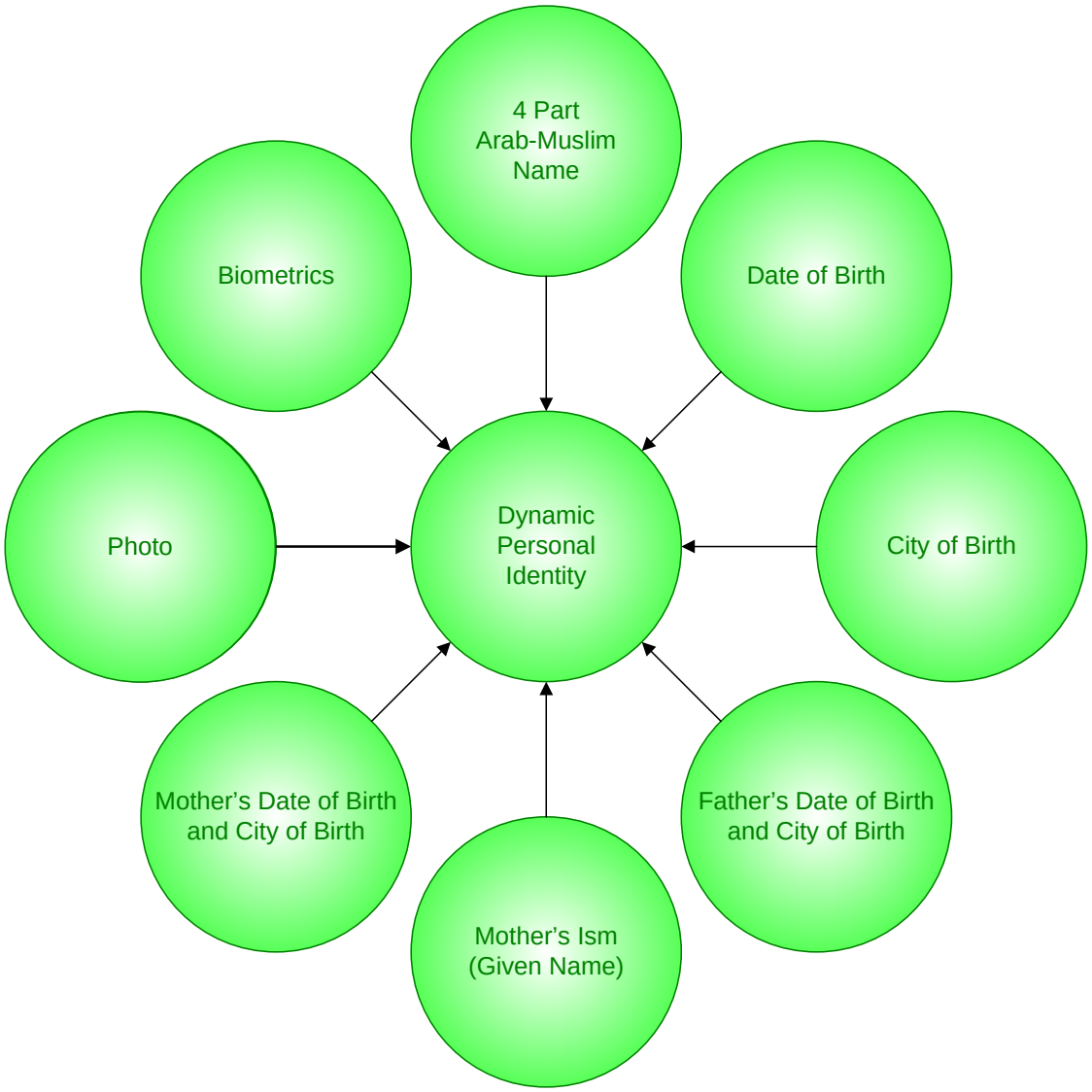


Figure 4. Components of Dynamic Personal Identity

It is thought that these same characteristics could be used globally with all visitors to the United States and could eventually be used within the United States to secure the personal identity of our own citizens. However, for the purposes of this project, we remain focused on Arab-Muslim persons wishing to enter the United States.

### 2. The Dynamic Identity Grid – A Conceptual Framework

The concept of the *Dynamic Identity Grid (DIG)* framework is heavily influenced by the U.S. Department of Defense's Global Information Grid (GIG).[222] The framework takes a net-centric approach to name-based personal identity that is based upon the recognition that information is critical to enabling better and faster strategic decisions based on timely and trusted information.[223] Increased knowledge flow through the *DIG* will allow for enhanced capabilities that are targeted at stopping terrorists and those that support them from entering or effectively operating within the United States. It is expected that the *DIG* will enable the United States Government to fully leverage the knowledge found within a person's *Dynamic Personal Identity*, eliminate organizational information stovepipes, and meet ever increasing demands for information about the personal identity of those wanting to enter the United States from foreign lands or those already living within the United States.

Solid support for such a framework is found in the combined National Security Presidential Directive 59 and Homeland Security Presidential Directive 24 that was issued on June 5, 2008.[224] The combined directives focus on biometrics for identification and screening in an effort to enhance national security.[225] However, they also recognize the importance of knowledge flow within the federal government and between itself and its partners. The directives explicitly call for the integration of interoperable systems and processes to enhance sharing of biometric and related biographical information (personal identity information) among federal agencies and between federal agencies and their foreign, state and local partners.[226] In addition to this most recent and specific combined

---

[222] For further information please see: Department of Defense, *Global Information Grid Architectural Vision* (Washington, DC: USGPO, 2007); and Department of Defense, *Capstone Requirements Document: Global Information Grid* (Washington, DC: USGPO, 2001).

[223] Department of Defense, *Global Information Grid Architectural Vision*, iii.

[224] "National Security Presidential Directive 59 and Homeland Security Presidential Directive 24," *The White House*, https://www.hsdl.org/homesec/docs/whitehouse/nps36-060608-01.pdf&code=f2c9e5bec3327f27afbc9741e318ef43 (accessed August 1, 2008).

[225] Ibid.

[226] Ibid.

directive, the framework finds its support in the multitude of homeland security related strategies and presidential directives issued since 9/11 that call for an increased use of technology and collaboration in the areas surrounding personal identity.[227]

The model includes a comprehensive information technology platform and a black core communications infrastructure among a variety of other core systems that are designed to provide seamless integrated systems for system defense, transactional and analytical processes, and system communications. Systems within each core will include data storage, transactional processors, and analytical processors. Sub-systems within each system will have specific functions designed to carry out specific processes such as consistent name transliteration; consistent and effective analysis and identification of name-based identities; and provision of real-time decision support and anomaly detection. The model developed by this project was terminated at the meta-level, leaving the development of the actual technological solutions to further research and development efforts. The meta-model was developed from an operational point of view and is aimed at providing guidance for engineers and application developers in their future research and development efforts.[228] A view of the meta-level total system architecture, including its information technology platform and communications infrastructure, is provided in Figure 5 below.

[227] 2008 U.S. Intelligence Community Information Sharing Strategy; 2007 National Strategy for Information Sharing; 2007 National Strategy for Homeland Security; 2006 National Strategy to Combat Terrorist Travel; 2006 National Strategy for Combating Terrorism; National Security Presidential Directive 46; Homeland Security Presidential Directives 2, 6, 11, 12, and 15; Executive Orders 12881, 13354 and 13388; and the 2005 Information Sharing Guidelines.

[228] Coleen Rolland, Modeling the Requirements Engineering Process, *Information Modeling and Knowledge Bases V: The Proceedings of the 3rd European-Japanese Seminar on Information Modeling and Knowledge Bases,* Held in Budapest, Hungary, May 31 – June 3, 1993, (Amsterdam: ISO Press, 1994), 86-97.

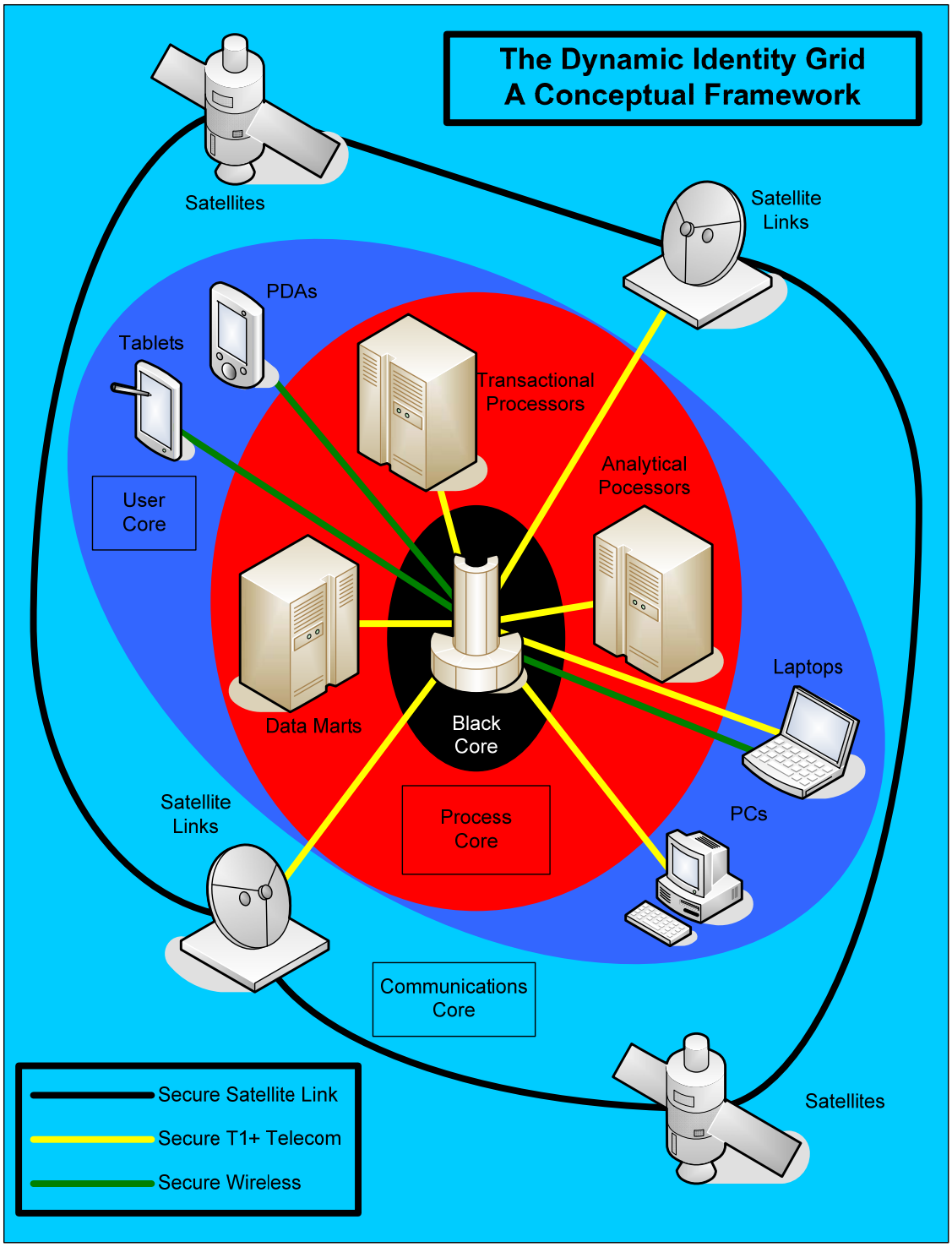


Figure 5. *DIG* Meta-Level Total System Conceptual Framework

The *DIG* will consist of information systems that enable access to, exchange, and use information and knowledge found throughout the United States Government to block

the travel and immigration of persons attempting to enter the U.S. that are terrorists or that support terrorist endeavors and to identify those already operating within its borders.[229] The current state of technologies related to personal identity are mired in a pool of legacy systems and newer technologies that exhibit varying degrees of interoperability and generally constrain access to much needed knowledge and information.[230] The framework presented here describes the *DIG* in general conceptual terms and is not intended to provide a full and technically accurate description. It is a starting point, not an end product, and is likely to take several years to fully develop.

The *DIG* is based upon a common Internet Protocol (IP) based packet communications layer that allows the system to be scaleable, robust and highly available to a multitude of human and computer users simultaneously.[231] The system is based on a need-to-share model that considers information and knowledge to be its strategic enterprise assets.[232] Its most common attributes are fully described in Table 3 – Dynamic Identity Grid Attributes, below.[233]

| Attribute | Description |
|---|---|
| Internet and World Wide Web Like | Adapts Internet and World Wide Web Constructs and Standards with enhancements for mobility and surety. |
| Secure and Available Information Transport | Edge to Edge Encryption That Is Hardened Against Denial of Service |
| Information/Data Protection and Surety | Producer/Publisher of Information Marks Info/Knowledge For Classification and Handling, Provides Provisions for Assuring Authenticity, Integrity and Non-Repudiation |
| Post In Parallel | Producer/Publisher Makes Info/Knowledge Visible and Accessible Without Delay |
| Smart Pull | Users Find and Pull Info/Knowledge Directly, Subscribe or Use Value Added Services |
| Information/Knowledge Centric | Information/Knowledge is Separate From Applications and Services, Minimizing the Need for Special or Proprietary Software |

[229] Department of Defense, *Global Information Grid Architectural Vision*, 1.

[230] Ibid.

[231] Ibid., 7.

[232] Ibid., 8.

[233] Ibid.

| Attribute | Description |
|---|---|
| Shared Applications and Services | Users Can Pull Multiple Applications to Access Data or Choose Same Applications When Collaborating |
| Trusted and Tailored Access | Access to Information Transport, Information/Knowledge, Applications/Services are Linked to Users Role, Identity and Technical Capability |
| Quality of Service | Tailored for Information Form: Knowledge, Voice, Still Imagery, Biometrics, Data and Collaboration |

Table 3. Dynamic Identity Grid Attributes

From the operational level, the *DIG* will consist of a diverse set of technological capabilities used to collect, process, store, deliver, protect and manage information and knowledge for its users as illustrated in Figure 6 below.[234]

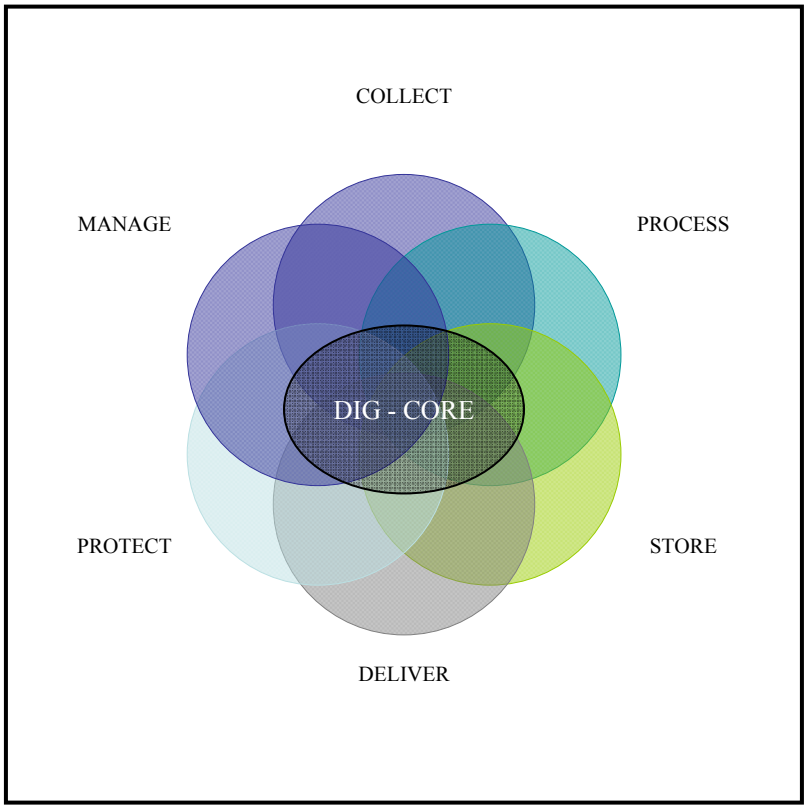


Figure 6. Dynamic Identity Grid Capabilities

[234] Department of Defense, *Global Information Grid Architectural Vision*, 11.

These processes are seamless for the user who benefits from the architecture's provision of transport, computing and information services at all classification levels.[235] Users will be responsible for capturing and posting information to the system as soon as it becomes available to them. Hypothetically, Consular Officers will post information on the identity of persons issued a new visa, Immigration and Customs Enforcement Agents will log the entrance and exit of foreign visitors and Border Patrol Agents will post information on arrests of illegal border crossers in real time. These posts will include the *Dynamic Personal Identity* characteristics of properly transliterated names, full names in the standard four name Arab-Muslim structure, and biometric identifiers in addition to other pertinent information or knowledge captured at each interaction. At the same time, the system will be continually completing knowledge-based analytics, including link analyses, alerting users to anomalies in real time.

Sharing of the knowledge and information within the *DIG* is enabled by a set of automated activities and capabilities that include meta-data information and knowledge tagging.[236] Meta-data will be attached to data sets to enable discovery, semantics, syntax and access control features that will allow other users to access the information they need.[237] The system will be highly dependent upon constant user interaction to both initially populate the systems data banks and to also continually improve its information and knowledge stores by adding more information and knowledge as it becomes available. Figure 7 shows a conceptual depiction of the *DIG's* single plane information and knowledge flow dynamics, as viewed from within the United States Government system.

---

[235] Department of Defense, *Global Information Grid Architectural Vision*, 11.

[236] Ibid., 13.

[237] Ibid.

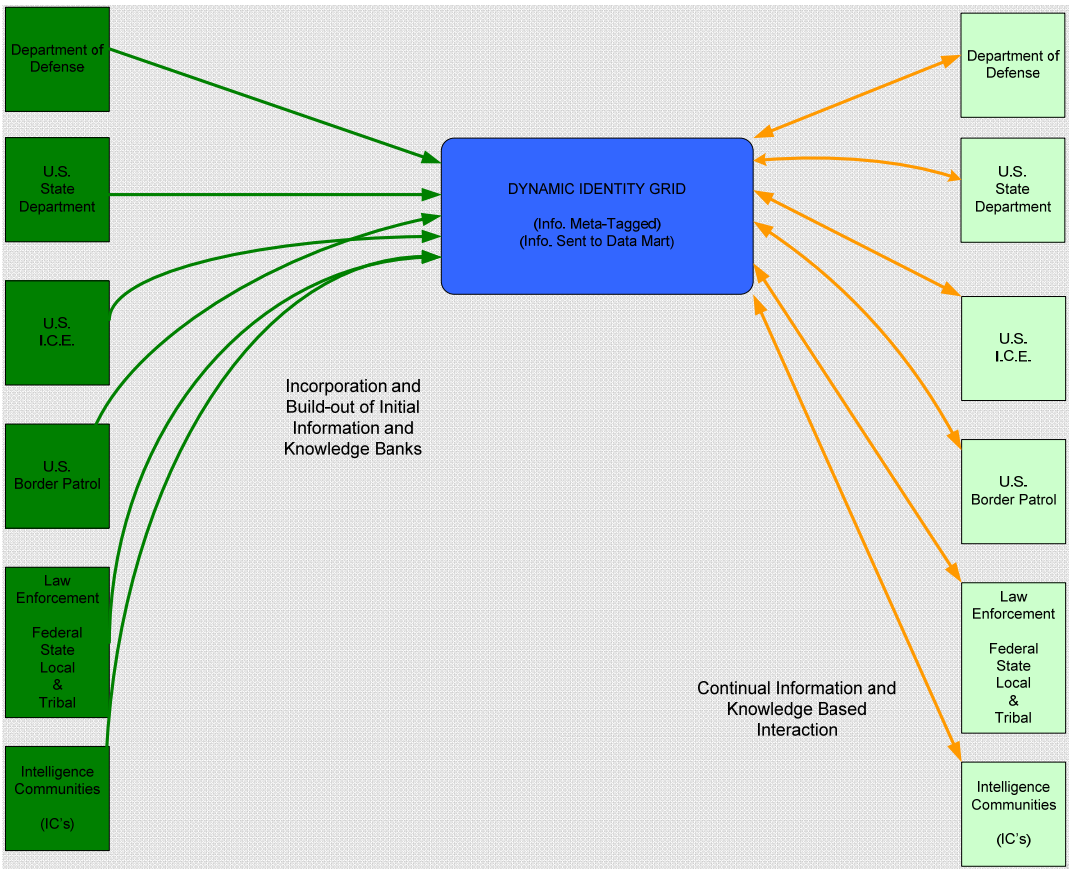


Figure 7. DIG Single Plane Flow Dynamics

Systematically, the *DIG* will have two main functional components, a mixed infrastructure and task specific applications, services and information. The *DIG* will support users through both human-computer interaction and automated machine to machine processing as illustrated in Figure 8. The User Core interacts with all system resources through the Black Core--as illustrated in Figure 5--and is routed to the Application Sub-Systems based on user needs. The Application Sub-Systems interact with the Support Sub-Systems Black Core to draw on Grid resources whether within the Support Sub-Systems or within the Process Core. This ensures user authentication and the integrity of the Grid, allowing multiple levels of authorization without separating knowledge, information and data from the Grid entirely. The Process Core is responsible for computer to computer interaction. It houses the overall analytic and transactional processes such as transliteration, biometric matching, anomaly detection and link

analysis. The Process Core also houses the Data Mart, which interacts with the Sub-System Data Stores to allow effective knowledge, information and data flow between all users.

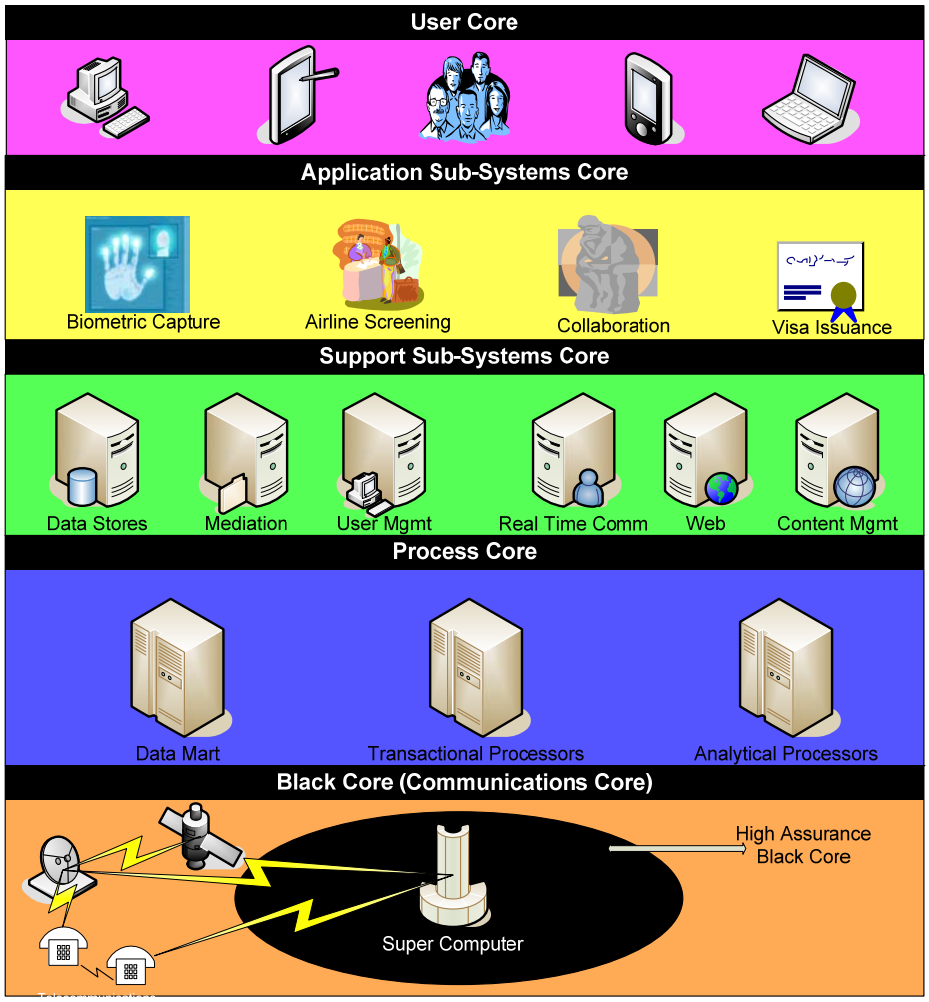


Figure 8. Layers of the Dynamic Identity Grid

As illustrated in Figure 8, the *Dynamic Identity Grid* has three main core systems and two main sub-system cores. The entire Grid is overlaid on the Black Core, a high security communications core that allows the system and its users to communicate across the globe through a variety of communications components, including satellite and hard wire telecommunications sub-systems. The Process Core contains the brains of the Grid and provides the information technology infrastructure necessary for data storage and

computer to computer processing and analysis that leads to new knowledge. The Process Core includes large computers for processing, analyzing and warehousing the data and knowledge used by the entire Grid and all of its computer and human users. The Support Sub-Systems Core is responsible for all of the sub-systems used by the Grid such as local data storage, systems mediation, user management, content management, internal web applications and real time communications between users and the Process Core. The Application Sub-Systems Core consists of all of the standalone applications that drive data collection and knowledge development. Such sub-systems are likely to include biometric collection and verification systems; standalone transliteration systems; massive data stores such as state Driver License systems and the Combined Terrorist Watch List; major interactive systems such as U.S. VISIT, the Consular Database, and NCIC; and many others that support the Grid's mission areas that are either in use today, in the developmental stages or those that are yet to be discovered. The User Core is made up of those technological devices employed by users to access the Grid and include desktop computers, laptop computers, tablets, PDAs and Smart Phones.

### 3. The Issue of Privacy

The main challenge to the implementation of an analytical knowledge-based program such as the *Dynamic Identity Grid* is expected to be based on perceived violations of individual privacy. A valid discussion about privacy cannot begin without a discussion of the definition of privacy itself. The Electronic Privacy Information Center (EPIC) and Privacy International contend that "definitions of privacy vary widely according to context and environment."[238] Their 2002 report provides the following discussion on the issue:

> In many countries, the concept has been fused with data protection, which interprets privacy in terms of management of personal information. Outside this rather strict context, privacy protection is frequently seen as a way of drawing the line at how far society can intrude into a person's affairs. The lack of a single definition should not imply that the issue lacks importance. As one writer has observed, "in one sense, all human rights

[238] *Privacy and Human Rights 2002: An International Survey of Privacy Laws and Developments* (Washington, DC: Electronic Privacy Information Center, 2002), 1-111.

> are aspects of the right to privacy." Robert Ellis Smith, editor of the *Privacy Journal*, defined privacy as "the desire by each of us for physical space where we can be free of interruption, intrusion, embarrassment, or accountability and the attempt to control the time and manner of disclosures of personal information about ourselves." According to Edward Bloustein, privacy is an interest of the human personality. It protects the inviolate personality, the individual's independence, dignity and integrity. According to Ruth Gavison, there are three elements in privacy: secrecy, anonymity and solitude. It is a state which can be lost, whether through the choice of the person in that state or through the action of another person.[239]

The author of this study clearly understands that the collection of personal information will always raise personal privacy concerns. This is a historical fact that similar proposals have faced in years prior to this study. In a 1996 report to the Connecticut Department of Social Services regarding personal identification information, James Laban documented that "In 1969, the American National Standards Institute (ANSI) proposed a standard national identifier. It was decided, however, that the level of distrust in government was such that was not a good idea" and, "in 1973, an Advisory Committee to the U.S. Department of Health, Education & Welfare concluded that a national identifier system should not be established"[240] Laban went on to conclude that, "in order for the government to be successful in implementing an effective identification system, like finger imaging, it needs to identify and address the public policy issues surrounding public resistance toward them."[241] It is assumed that the implementation of the *Dynamic Identity Grid* will come under the same scrutiny that Laban described in his 1996 work.

---

[239] Adapted from: *Privacy and Human Rights 2002: An International Survey of Privacy Laws and Developments* (Washington, DC: Electronic Privacy Information Center, 2002), 1-111; For further information reference the report or these citations from the report: James Michael, *Privacy and Human Rights* (UNESCO, 1994), 1; Simon Davies, *Big Brother: Britain's Web of Surveillance and the New Technological Order 23* (Pan, 1996); Fernando Volio, "Legal personality, privacy and the family" in Henkin (ed.), *The International Bill of Rights* (Columbia University Press, 1981); Robert Ellis Smith, *Ben Franklin's Web Site* (Sheridan Books, 2000); "Privacy as an Aspect of Human Dignity," *New York University Law Review* 39 (1964): 971; "Privacy and the Limits of Law," *Yale Law Journal* 89 (1980): 421, 428.

[240] Connecticut Department of Social Services, *Privacy Issues Surrounding Personal Identification Systems*, by James Laban, 1996, www.ct.gov/dss/lib/dss/PDFs/diprivac.pdf, (accessed December 10, 2007).

[241] Ibid.

In a more modern context, a 2006 brief issued by the National Association of State Chief Information Officers (NASCIO) concluded that "privacy is a defining issue of the day for both the public and private sectors."[242] The underlying concerns of modern privacy discussions do not seem to be related to the collection of the information so much as the improper storage or use of the information. For example, the NASCIO brief states "citizens are now aware of data breaches, identity theft and the risks that can result from personal information finding its way into ill-intended hands."[243] This tends to lead one to believe that the modern discussion relates more to information security than information privacy.

While a right to privacy is not explicitly guaranteed in the United States Constitution, a 1965 decision of the United States Supreme Court held that privacy is an important issue. The Supreme Court recognized this by providing protection to the public through their decision in Griswold versus Connecticut regarding marital privacy.[244] In this decision, the majority opinion agreed that there was no strict right to privacy, but that it was contained in the "penumbras" of other constitutional protections.[245] The Griswold decision is the historical basis for privacy arguments in the United States today. From an international perspective, the 2002 report issued by EPIC and Privacy International states that "privacy is a fundamental human right" and that "it is protected in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and in many other international and regional human rights treaties."

Privacy concerns are highly important to this project, because the privacy discussion is driven by an environment of increased information and knowledge sharing across traditional agency and governmental boundaries and the ease with which information can be collected, compiled, manipulated, used and transmitted

---

[242] National Association of State Chief Information Officers, *Research Brief: Keeping Citizen Trust: What Can a State CIO Do to Protect Privacy?*, www.nascio.org (accessed December 1, 2007).

[243] Ibid.

[244] Griswold v. Connecticut from Wikipedia, http://en.wikipedia.org/wiki/Griswold_v._Connecticut (accessed December 10, 2007).

[245] Ibid.

technologically.[246] According to NASCIO, "the nature of the privacy discussion is evolving and has become increasingly complex." A discussion about information and knowledge collection and sharing would not be complete without a discussion of ways to ensure privacy.

There are many arguments about the proper way to ensure privacy. George T. Duncan argues for the use of an RU Confidentiality Map to ensure privacy.[247] Joel R. Reidenberg argues that "data privacy is generally accepted internationally as a fundamental human right" and that the United States should adopt models similar to those used in the European Union to ensure privacy of personal data.[248] Even the United States Department of Justice has developed a Privacy Policy Development Guide to foster a balance between justice information sharing and privacy concerns.[249] However, this project is unique in that it deals exclusively with non-immigrant visitors to the United States' homeland. As such, non-immigrant visitors are not afforded the protections of the Privacy Act.[250] The Privacy Act does require the creation of a System of Records Notice for any system of records that is maintained by a United States federal government agency.[251] It has been the past practice of United States Government agencies to apply the same rules and protections to all information maintained within their systems, including information on individuals other than U.S. citizens and Lawful Permanent Residents.[252] Due to the fact that the proposed conceptual framework within this project is projected to become an integrated tool, a system of systems, it is proposed that the system adopt the same protections already provided by previously integrated systems

---

[246] National Association of State Chief Information Officers, *Research Brief: Keeping Citizen Trust: What Can a State CIO Do to Protect Privacy?*, 2.

[247] John Podesta, Peter M. Shane and Richard C. Leone, *A Little Knowledge: Privacy, Security and Public Information after September 11* (New York: Century Foundation Press, 2004,) 1-159.

[248] Ibid., 94.

[249] United States Department of Justice, *Privacy Policy Development Guide and Implementation Templates* (Washington, DC: United States Government Printing Office, 2006), 1-146.

[250] United States Department of Homeland Security, *US-VISIT Program, Increment 1 Privacy Impact Statement* (Washington, DC: United States Government Printing Office, 2003), 1-13.

[251] United States Department of Homeland Security, *Discussions of Public Comments Received on the Automated Targeting System: System of Records Notice* (Washington, DC: US-DHS, 2006), 1-25.

[252] United States Department of Homeland Security, *US-VISIT Program, Increment 1 Privacy Impact Statement*, 1.

within the U.S. Government. It is proposed that the *Dynamic Identity Grid* use the US-VISIT as its model privacy program and to institute access controls similar to those employed by the Department of Defense's Global Information Grid.

The US-VISIT program has a robust privacy protection program to secure individual information such as name, date of birth, gender, citizenship, passport number and address.[253] The information collected by US-VISIT is done so to verify the identity of covered individuals who enter or leave the United States.[254] The implementation of the *Dynamic Identity Grid* as the overarching framework to the US-VISIT system allows for easy implementation of its privacy protections. As with all US-VISIT related information collection, the admission of individuals subject to the requirements of the program will be contingent upon submission of the required information.[255] Those that wished not to provide information requested under the *Dynamic Identity Grid* system would not be admitted to the United States or would face removal proceedings under similar guidelines that the US-VISIT program currently has in place.[256] The US-VISIT system currently has maintenance and administrative controls on access to the data, including policies on subjects such as with whom information will be shared, how the information will be secured, how information will be collected, how information will be used and disclosed, how information will be processed and how information will be retained and destroyed.[257] These are vetted and approved practices that are currently in place for similar processes and are easily adaptable to the knowledge flow processes of the *DIG*. In addition to these protections, the idea of a "black core," as described earlier in the Chapter, will ensure proper human user interface with personal information.

In conclusion, issues related to personal privacy in relation to a project that is intended to collect, store and analyze personal information are naturally expected. However, the protection of the United States' homeland is recognized by Congress as a

---

[253] United States Department of Homeland Security, *US-VISIT Program, Increment 1 Privacy Impact Statement*, 1.

[254] Ibid., 2.

[255] Ibid.

[256] Ibid.

[257] Ibid., 5-8.

paramount issue when pitted against claims of privacy violations by non-immigrant visitors to the United States. Even with this in mind, past practice of federal agencies has been to protect the information of foreign nationals as if it was the information of a United States citizen. As such, the proposed implementation of the *DIG* as an overarching framework for other government systems should not be any less subject to the constraints imposed upon these programs by their host agencies.

### 4. Strategy for Development and Implementation

The development of a bold conceptual technological framework that defies traditional operational norms of the United States Federal Government will not be accepted without a comprehensive strategy for presentation of the subject to those appropriating funds for its development and implementation. Equally important is a strong sense of what lays ahead, the likely pitfalls for leaders as they attempt to develop and implement the framework and a comprehensive strategy for avoiding them. The proposed strategy presented here, like the conceptual framework itself, will be unique in that its main foundation will be cast from the latest texts in business theory while remaining balanced by more traditional approaches. This proposed strategy is not intended to be as rigorous as the fully researched conceptual framework presented earlier in the chapter, but instead it is intended to serve as a catalyst for further development and implementation of the concepts. This strategy is provided as a way forward from the academic conclusions of the research for those that may wish to operationalize its findings.

Bold new concepts emerge from unlikely places and most often catch many persons by surprise. They gain power and influence quickly when put into action, often resulting in outcomes much greater than their creators could have imagined. Recent examples include eBay, Napster, Facebook, MySpace, and even Al Qaeda. All of these notions have a similar quality that is a key to developing and implementing the concept of the *Dynamic Identity Grid (DIG)*. Each is centered on the single overriding principle

of decentralization.[258] For the *DIG,* decentralization is a key component and is centered on laws and governmental policies, processes and procedures as well as governmental agencies, networks and technologies.

As discussed in Chapter II, the current disparate roles enjoyed by multiple governmental agencies surrounding name-based personal identity will be decentralized by the development of the *DIG.* By leveraging the power of technology, current stove-piped legacy systems will become a lesson from the past of how centralization of information, systems and processes reduces efficiency and increases the chances for privacy invasion. By decentralizing the roles of various government agencies and technological programs and combining the knowledge found within personal identity with technology, it is hoped that the *DIG* will meet with similar success as the other decentralized concepts discussed above. Such a decentralized program is expected to improve the U.S. Government's capability to defend its homeland while improving levels of personal privacy for innocent citizens and visitors of the United States. Decentralization is a powerful hidden force - "The harder you fight this force, the stronger it gets. The more chaotic it seems, the more resilient it is. The more you try to control it, the more un-predictable it becomes."[259] It is thought that, through the power of decentralized "dynamic" personal identity, dangerous groups that depend on kinship for trust amongst its members may be unraveled and defeated. In this context, the same principle that these groups use to grow stronger can also be employed to their demise.

Current personal identity practices spread across various government agencies and supported by disparate technological systems are locked in an epic competition to be the key component in unraveling terrorist networks. One of the most recent manifestations of this battle of stove-piped systems is the emergence of biometrics as a tool to secure personal identity. The use of biometrics seems to be hailed as the Holy Grail in securing the U.S. homeland against unwanted terrorist invasion. However, the

[258] Ori Brafman and Rod A. Beckstrom, *The Starfish and the Spider* (New York: Portfolio, 2006).

[259] Ibid., 6.

concept of a *Dynamic Identity Grid* merely makes the use of biometric technology a decentralized component of the overall framework, seeking to leverage its knowledge for all users and not depending on it as a sole source of security for the entire system.

For a hypothetical example of how biometrics becomes a decentralized component of the overall system, we will look at the following scenario. The US-VISIT program confirms that a person entering the United States at New York's Kennedy Airport on a tourist Visa is the same person that applied for the Visa in Karachi four months earlier through a biometric match. This information is shared between the Department of State and components of the Department of Homeland Security in a stove-piped system. Currently, this is where the transaction ends. However, using the *DIG*, a seemingly honest applicant for a tourist Visa is linked to his brother via his *Dynamic Personal Identity* and the *DIG* leverages this information in real time, finding that the subject's brother was detained by the Department of Defense in Iraq and was sent to Guantanamo Bay for acts of terrorism against the United States a month after the subject's tourist Visa was issued. Knowledge stored in the *DIG's Dynamic Identity Mall* is accessed by the computer to computer *Dynamic Identity Analytics* component and finds that interrogations at Guantanamo found several family members in New York and Karachi were planning an attack within the United States. This alerts the system to anomalistic events based on its anomaly detection assets. The anomaly detection assets, seeing that a family member of a known terrorist is attempting to enter the United States as a tourist, notifies the Immigration human user interacting with the individual in New York to gather more information about the subject's travel plans, conduct a thorough search of the subject's belongings and then deny him entry to the United States. The human interaction reveals information about a cousin already living in New York, suspicious materials in the subject's suitcase and eventually unravels a terrorist cell in Brooklyn made up of members from three families all linked by their *Dynamic Identities* during a Joint Terrorism Task Force follow up investigation.

### *a. The Dynamic Identity Grid: A Blue Ocean Perspective*

In the spirit of *Blue Ocean Strategy*, the conceptual framework for *DIG* was developed in an attempt to create uncontested market space, making the competitive arena of individual components of personal identity irrelevant.[260] Market space, in this sense, is meant to refer to an increase in security through leveraged knowledge versus maintenance of the status quo evident in various stove-piped systems. As described by Kim and Mauborgne, "Red Oceans" represent known market space and "Blue Oceans" represent those approaches and concepts that remain unknown.[261] In red oceans, boundaries are known and accepted and the competitive rules of the game are known.[262] This is the current state of personal identity for persons entering the United States. Due to the ethnocentrically-based collection of personal names, lack of focus regarding the kinship element inherit to terrorist organizations, and the stove-piped practices and technologies that make up the U.S. personal identity system; terrorists are able to effectively compete against the system, bloodying the waters of personal identity and making it nearly impossible for U.S. authorities to prevent their entrance into the United States. As discussed in Chapter II, all nineteen 9/11 terrorists entered the United States legally. It is now known that several were linked to terrorism prior to 9/11, but "red ocean" stove-piped systems and lack of real time leveragable knowledge made it virtually impossible for links to be established within the intelligence and law enforcement communities. By making a bold move towards the blue ocean of the *DIG*, U.S. officials can move beyond traditional conceptual boundaries and re-set the rules of the game.[263] By building a decentralized system of systems, understanding and leveraging the information contained on a person's *Dynamic Personal Identity*, and destroying stovepipe systems that fail to communicate across agency boundaries, it is hoped that future terrorist acts can be avoided. The development of tactics to circumvent personal identity

---

[260] W. Chan Kim and Renee Mauborgne, *Blue Ocean Strategy* (Boston: HBS Press, 2005).

[261] Ibid., 4.

[262] Ibid.

[263] Ibid.

systems will never stand still and, like industry, they will continually evolve.[264] As such, the *DIG* will not remain a blue ocean without continual enhancement. Once the framework is fully developed and implemented, it will be necessary to continually improve upon the original product to leave its terrorist competitors behind. By continuously creating a broader blue ocean through enhancement and improvement, the *DIG* can remain in new, uncontested market space. In other words, future leaders should not rely upon the *DIG's* ability to have a meaningful impact on counter-terrorism without continuous improvement. This is readily apparent with the current personal identity practices within the United States that were shown to be uncompetitive in the months leading up to the 9/11 attacks.

The current practice of developing new un-connected and un-integrated technologies to deal with the personal identity dilemma causes the U.S. Government to remain caught in a classic red ocean approach. In this red ocean approach the federal system is "racing to beat the competition by building a defensible position within the existing competitive order."[265] In contrast, blue oceans are created by ignoring the current rules of order by following a different strategic logic called "value innovation."[266] Instead of focusing on the short term defeat of its competition, value innovation makes the competition irrelevant by creating a leap in value (leveraged knowledge) for buyers (the citizenry).[267] By placing an equal emphasis on value and innovation, the value-cost trade-off is eliminated and a blue ocean of market space is created.[268] In the case of *DIG*, the cost of death, injury and economic damage (risk to citizens and the economy) delivered by terrorists is driven down and the value of leveraged knowledge is driven up, creating the value innovation of early detection of terrorists and their supporters (see Figure 9).

---

[264] Kim and Mauborgne, *Blue Ocean Strategy*, 6.

[265] Ibid., 12.

[266] Ibid.

[267] Ibid.

[268] Ibid., 13-14.

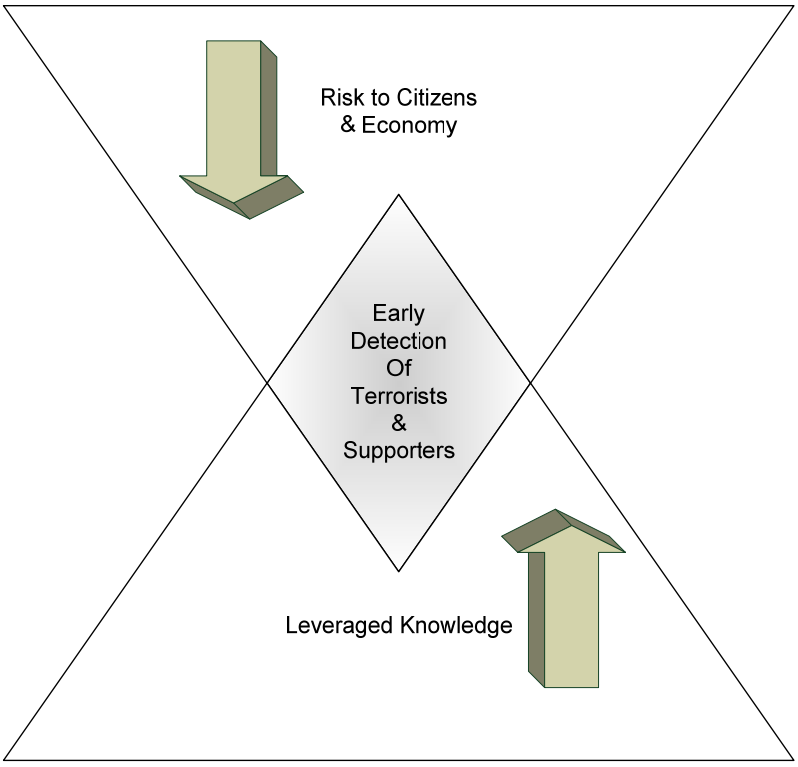


Figure 9. Value-Cost Trade-Off of the *DIG*

By creating value innovation, homeland security leaders can avoid the trap of environmental determinism. That is, they can avoid the assumption that structural conditions are given and competition must occur within them.[269]

To build a compelling "Blue Ocean Strategy," a diagnostic and action framework called a "Strategy Canvas" is developed that serves two purposes.[270] It captures the current state of play in the known market space, allowing you to plot the value curve of the competition, and it allows for a depiction of the value proposition and value innovation being proposed.[271] Prior to plotting value curves on the strategy canvas, a set of principal factors must be developed. Principal factors are the range of issues for competition and investment within a red ocean.[272] Principal factors are developed through the four action framework that asks four key questions to challenge the strategic

[269] Kim and Mauborgne, *Blue Ocean Strategy*, 17.

[270] Ibid., 25.

[271] Ibid., 25-28.

[272] Ibid., 25-26.

logic of the status quo. First, it asks which factors, that the industry takes for granted, should be eliminated. Second, it asks which factors should be reduced below the industry standard. Third, it asks which factors should be raised above the industry standard. Finally, it asks which factors should be created that the industry has never offered (see Figure 10).[273]

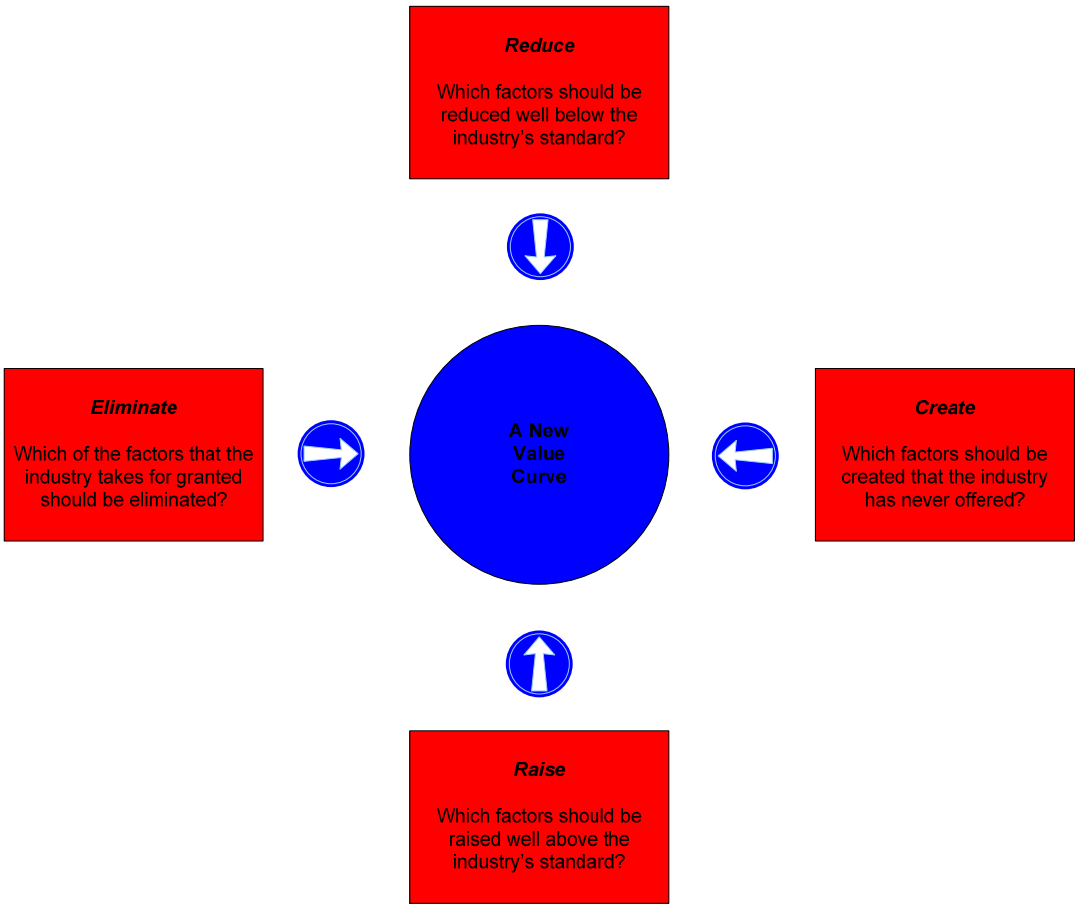


Figure 10. Eliminate-Raise-Reduce-Create Model

[273] Kim and Mauborgne, *Blue Ocean Strategy*, 29-30.

In order to effectively determine the answers to the four questions within the four actions framework, the Eliminate-Raise-Reduce-Create Grid is used. Use of the ERRC Grid pushes for answers and action on the four questions, creating a new value curve.[274] In the case of the *Dynamic Identity Grid*, the Blue Ocean ERRC Grid and Strategy Canvas appear below (See Figures 11 and 12).

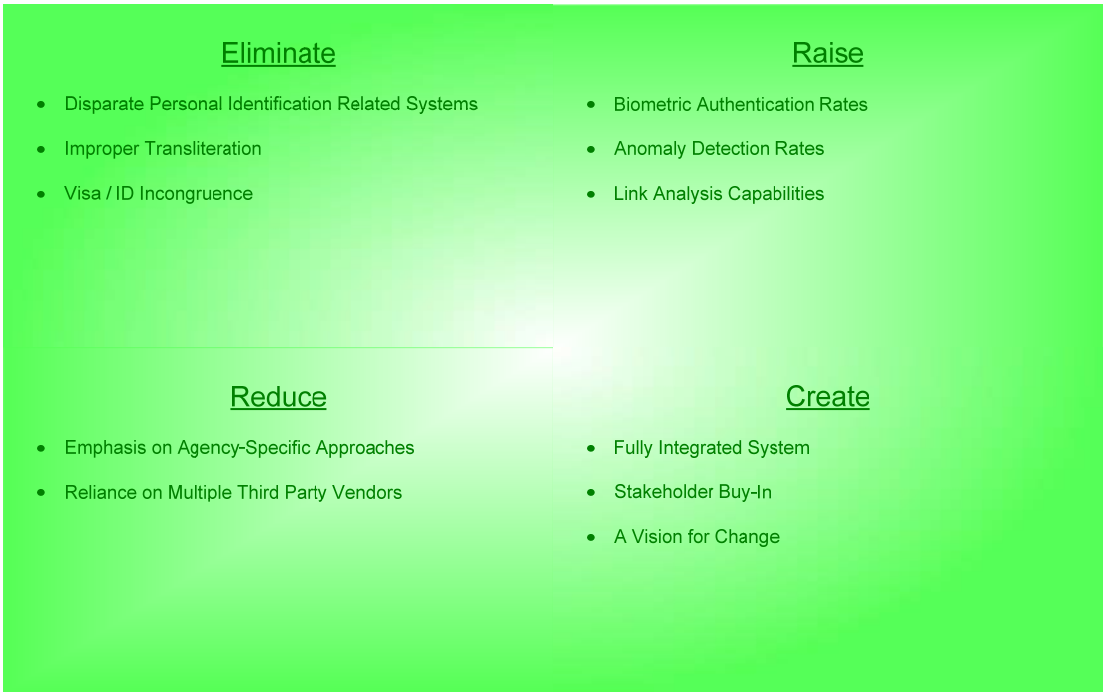


Figure 11. Eliminate-Reduce-Raise Create Grid for the Dynamic Identity Grid

[274] Kim and Mauborgne, *Blue Ocean Strategy*, 35-36.

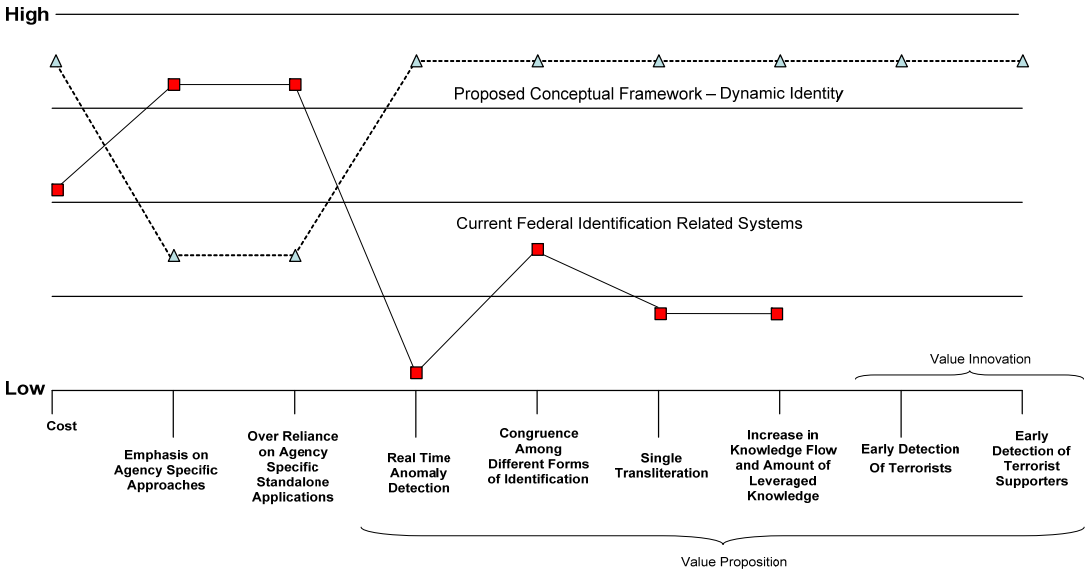


Figure 12. Dynamic Identity Grid Strategy Canvas

As presented above, the strategy canvas for the *DIG* exhibits characteristics of a "good" strategy by exhibiting focus and divergence.[275] It focuses on building knowledge and the dynamic nature of name-based personal identities and is divergent from the accepted norms found with the U.S. Government's current approach to personal identity. In addition, a compelling tagline such as "Enhancing the Security of America's Homeland through the Dynamics of Personal Identity" can be developed to meet the remaining requirement of a "good strategy," as described by Kim and Mabourgne.[276] According to them, a strategy without these qualities is likely muddled, undifferentiated, and cost prohibitive; with the more positive qualities described above serving as a litmus test of the viability of a blue ocean idea.[277] To be focused, a blue ocean strategy must emphasize a minimum number of factors that reduce overall investment; knowledge and dynamics of identity. To be divergent, the value curve of a blue ocean strategy must stand apart from the status quo; current stove-piped U.S.

[275] Kim and Mauborgne, *Blue Ocean Strategy*, 37-41.

[276] Ibid.

[277] Ibid., 37.

Government practices versus the overarching approach of the *Dynamic Identity Grid*. Finally, to be effective, a blue ocean strategy must have a compelling tag line or, at least, it should engender one, as presented above.[278] When a value curve lacks focus, it is too costly and complex; when it lacks divergence, the strategy is clearly one that is "me-too" and it will not stand apart; and when it lacks a compelling tag line, it is likely an internally driven innovation just for the sake of innovating.

Kim and Mauborgne recognize four organizational hurdles to successful strategy execution: cognitive hurdles, political hurdles, motivational hurdles, and resource hurdles. See Figure 13. Like sharks, these hurdles surround a blue ocean idea and attempt to destroy its innovative impact.

[278] Kim and Mauborgne, *Blue Ocean Strategy*, 39-40.

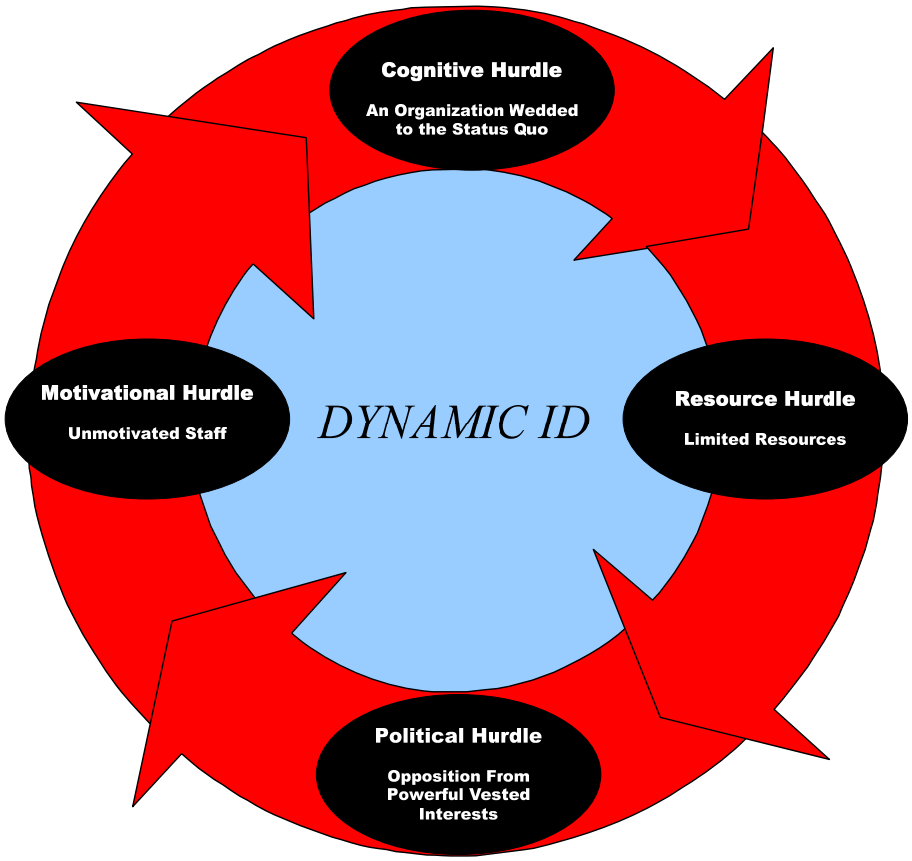


Figure 13. Hurdles to the Dynamic Identity Grid

The hurdles can be overcome by organizations that make quick fundamental changes based on the creation of an epidemic movement toward an idea. The movement is engendered by the redirection of the beliefs and energies of a critical mass of people within the organization with the key to such epidemic movements being concentration, not diffusion.[279] Building the *Dynamic Identity Grid* will be a massive challenge and it would be easy to fall victim to any of the four hurdles mentioned above.

[279] Kim and Mauborgne, *Blue Ocean Strategy*, 151.

Conventional wisdom would contend that such a massive challenge would require an organization to put forth an equally massive response, achieving gains by proportional investments in time and resources.[280] However, the move towards the *DIG* will require a different kind of involvement by its user stakeholders on order to conserve resources and reduce the time required to fully develop all of its systems. This will allow stakeholders to focus their time on identifying and leveraging the factors of disproportionate influence within what we will discuss as the *Dynamic Identity Mega-Community* later in this text.[281]

The disproportionate influence factors, people, acts and activities that exercise a disproportionate influence on overall group performance, must be identified and leveraged in advance of any formal strategic development or implementation processes.[282] Someone must direct the work of the *Dynamic Identity Mega-Community* and focus them on the following key points to ensure success.[283]

- Identifying the factors or acts that exercise a disproportionately positive influence on breaking the status quo.
- Identifying the processes and systems that will provide a maximum return on investment.
- Identifying and motivating key players to aggressively pursue change.
- Identifying and eliminating political roadblocks.

The cognitive hurdle to strategy execution involves perpetuation of the status quo within an organization. The mistake of most leaders is to focus their time and energy on pointing to the numbers and asking their organization to set higher goals and achieve better results.[284] This is the overall problem within the disparate organizations involved in the personal identity continuum. All of these organizations are setting their own goals, developing their own programs and processes and asking their employees to meet or exceed stove-piped benchmarks. In opposition, the *Dynamic Identity Mega-*

---

[280] Kim and Mauborgne, *Blue Ocean Strategy*, 151.

[281] See Next Section Titled The Dynamic Identity Mega-Community.

[282] Kim and Mauborgne, *Blue Ocean Strategy*, 151.

[283] Ibid.

[284] Ibid.

*Community* should focus its efforts on the act of disproportionate influence by making people see and experience the harsh reality of homeland security failures related to personal identity firsthand.[285] It is the desire of the author that this study may even serve as a catalyst for such an argument. By doing so, the Mega-Community will be able to impart the tacit knowledge necessary to positively influence the key stakeholders within it, inspiring a fast change that is internally driven of each participant's own accord.[286] Consider the example in Chapter II regarding the 9/11 hijackers, "nineteen 9/11 hijackers used 364 aliases, including different spellings of their names and noms de guerre."[287] A comprehensive technological system of systems that prevented the use of 364 different aliases, identified familial links between suspects terrorists and supported decision making of U.S. Government employees may have been able to prevent the 9/11 attacks!

After jumping the cognitive hurdle through acceptance of the need for a strategic shift, leaders are most often met with the reality of limited resources.[288] In the current homeland security environment, this is likely to be true. Dwindling homeland security funds, the current economic downturn and a new executive will likely make this hurdle quite high. By concentrating on multiplying the resources within the stove-piped systems that surround personal identity, the *Dynamic Identity Mega-Community* can capitalize on limited resources through its collaborative efforts. Rather than focusing on multiple solutions to the same issues, the *Dynamic Identity Mega-Community* can avoid the perpetual trap of high resource input for relatively low performance impact. By trading under-utilized resources or re-directing over-utilized resources to the *Dynamic Identity Mega-Community*, leaders from the various components of the mega-community can fill resource gaps and eliminate wasteful spending. This "horse trading" of resources benefits the mega-community as a whole by filling gaps and saving dollars across the board.[289] By determining which actions consume the greatest resources with little impact

---

[285] Kim and Mauborgne, *Blue Ocean Strategy*, 152.

[286] Ibid.

[287] Eldridge, et al., *9/11 and Terrorist Travel*, 1-241.

[288] Kim and Mauborgne, *Blue Ocean Strategy*, 156.

[289] Ibid.

and which activities have the greatest impact, but remain resource starved, organizations rapidly gain insight into how they might free up low return resources and redirect them to high impact projects. This type of focus would allow the *Dynamic Identity Mega-Community* to lower costs and create higher value simultaneously.[290] This would be true for actual positions within the various organizations and for similar or duplicative third party consultant and vendor contracts.

The greatest and most innovative ideas are regularly eaten alive by politics, intrigue and plotting.[291] If organizational politics are an inescapable reality, the politics of a mega-community are surely to be a tough hurdle to overcome. Powerful vested interests such as strong inter-governmental rivalries, third party consultant and vendor rivalries, advocacy groups and the pure political nature of the U.S. Government bureaucracy will surely resist the impending change required to fully develop the concept of a *DIG*. Recognizing these political hurdles and understanding that the more likely change becomes, the more fierce and vocal opponents will become is a major key to success.[292] To overcome political forces, the proponents of the *DIG* will have to leverage its supporters, silence its cynics and choose a trusted advisor to guide their top management team.[293]

It will be of utmost importance to choose a trusted advisor that is well respected and, in a sense, feared for his ability to identify those who will fight or silently attempt to sabotage the effort.[294] Simultaneously, the trusted advisor will help the management team identify those supporters within the system that will naturally align with and gain the most from a strategic shift to the *Dynamic Identity Grid*.[295] By building a coalition of support, the management team will effectively silence the cynics that attempt to destroy innovation. By choosing someone to advise and guide the

---

[290] Kim and Mauborgne, *Blue Ocean Strategy*, 156.

[291] Ibid., 165.

[292] Ibid., 166.

[293] Ibid.

[294] Ibid., 167.

[295] Ibid.

*Dynamic Identity Mega-Community* around the potholes and political opposition that it will face, the team will avoid sure political failure. A coalition of the willing will isolate and make irrelevant those forces attempting to stop a major strategic shift. A key angel in disguise for the *DIG* is likely the American Civil Liberties Union (ACLU). Securing the support of the ACLU in the beginning would likely diffuse other advocacy groups that may attempt to derail the project. As discussed earlier in this chapter, privacy concerns will be a key political hurdle to overcome.

### *b. The Dynamic Identity Grid Mega-Community*

Translating thought into action, actually executing strategy, is a challenge for any organization.[296] The case of the *DIG* is no exception and is likely even more problematic than most, due to its perceived impact on a large and diverse community of stakeholders. In the past, the theory and practice of strategic planning has been focused on enhancing the performance of single organizations.[297] As more organizations and stakeholders become involved in a project, achieving high levels of effective collaboration become much harder.[298] Developing the *DIG* will test the limits of this concept and will require a great deal of effort to create the vision, goals, and actions necessary for currently autonomous stakeholders to achieve collaborative success.[299] No single governmental organization within the United States will be able to fully develop the *Dynamic Identity Grid* on its own. However, by viewing the *DIG* conceptual framework through the Theory of Collaborative Advantage (TOCA) one can start to see that the conceptual framework can be fully realized. TOCA allows leaders to benefit from the "synergistic outcome gained through collaboration in which something is achieved that could not have been achieved by any organization acting alone."[300] This synergistic

---

[296] Kim and Mauborgne, *Blue Ocean Strategy*, 147.

[297] John M. Bryson, *Strategic Planning for Public and Nonprofit Organizations* (San Francisco: Jossey-Bass, 2004), 377.

[298] Bryson, *Strategic Planning for Public and Nonprofit Organizations,* 377.

[299] Ibid., 378.

[300] C. Huxam, "Theorizing Collaboration Practice." *Public Management Review* 5, no. 3, (2003): 401-423. As quoted in *Strategic Planning for Public and Nonprofit Organizations*, 378.

outcome is termed *collaborative advantage*.[301] TOCA includes the overarching challenge of pitting *collaborative advantage* against *collaborative inertia* and the underlying challenges of leadership, managing aims, building trust, managing power, membership structures, appropriate working processes, accountability, commitment and determination, resources, democracy, equality and compromise.[302] However, even the principles of TOCA fall short, because they do not seem to take into account the dynamics of the mega-community necessary to tackle such a complex issue of global importance. The use of a mega-community strategy allows leaders to seek optimization over mere collaboration.

However, what is a mega-community? While collaboration is appropriate for mega-community formation, optimization through negotiation is the key to controlling the operations of a large group of diverse stakeholders once they are past the point of initial convergence.[303] Critical global issues like the ones discussed in this thesis are concerns that are mutual to many organizations and can only be properly addressed in a shared manner providing value for stakeholders from government, business and civil society.[304] Such tri-sector engagement can provide a dynamic balance that is grounded in better communication and cross-organizational structures.[305] Drawing heavily on the fields of network theory, group dynamics, and behavioral economics, the idea of tri-sector Mega-communities provides a model of collective leadership in which no single leader or organization is in charge.[306] By developing successful partnerships across all three sectors, leaders from all of the organizations involved work within the mega-community to address complex issues and increase decision velocity.[307] Leaders have come to the conclusion that "for any complex situation anywhere in the world, it's

---

[301] Huxam, "Theorizing Collaboration Practice," 378.

[302] Ibid.

[303] Mark Gerencser, Reginald Van Lee, Fernando Nepalitano and Christopher Kelly, *Megacommunities: How Leaders of Government, Business and Non-Profits Can Tackle Today's Global Challenges Together* (New York: Palgrave MacMillan, 2008), 100.

[304] Ibid., 16.

[305] Ibid., 17-18.

[306] Ibid., 18-20.

[307] Ibid., 15-20.

become obvious that there is no one authority – whether in the form of a leader, an organization, a command operation, or a rescue squad – that can single handedly save the day."[308] The problems found within the organizations that concern themselves with personal identity are no exception to this rule. In fact, while regularly seen as a government only issue by those within government, the private sector and civil society are intimately intertwined throughout the programs and processes associated with personal identity. To think that the U.S. Government could single handedly solve the problems associated with personal identity is preposterous. Even more ludicrous is the thought that a single unit of the federal government could do so. By changing the planning processes and relationships among the various groups that have a vested interest in personal identity, a *Dynamic Identity Mega-Community* could be formed.[309]

Mega-communities are based upon the idea that communities of organizations from the private, government and civil sectors can be vehicles for large-scale change that is both feasible and needed.[310] The leaders of these organizations deliberately come together across national, organizational and sectoral boundaries to reach goals that they cannot achieve alone.[311] In the case of the *Dynamic Identity Mega-Community* it is hoped that representatives from the Department of State, Intelligence Community, various State Licensing Agencies, ACLU, Government Contractors, Private Sector Vendors and other vested stakeholders will come together to develop and implement the *DIG* conceptual framework presented here. Such a mega-community would enable the various stakeholders to recognize their common ground and goals and would allow those involved from all three sectors to reduce the overwhelming complexity of personal identity without any one of them dominating the work of the group.[312] Taking this concept further, a discussion of how a mega-community operates follows below.

---

[308] Gerencser, Van Lee, Nepalitano and Kelly, *Megacommunities: How Leaders of Government, Business and Non-Profits Can Tackle Today's Global Challenges Together*, 26.

[309] Ibid., 27.

[310] Ibid., 28.

[311] Ibid.

[312] Ibid., 46.

The mega-community concept thrives on the "dynamic tension" that exists between business, government and civil society, gaining energy and excitement from the sectors as they operate within the same space simultaneously.[313] Within a healthy mega-community the sectors maintain their balance by pushing and pulling at each other through levers of influence.[314] Protocols and principles such as regulations, boycotts and voting serve as levers of influence between the sectors and work in both directions to maintain stability among the participants and sharpening each sector's sense of their own objectives within the overall mission of the community (see Figure 14).[315]

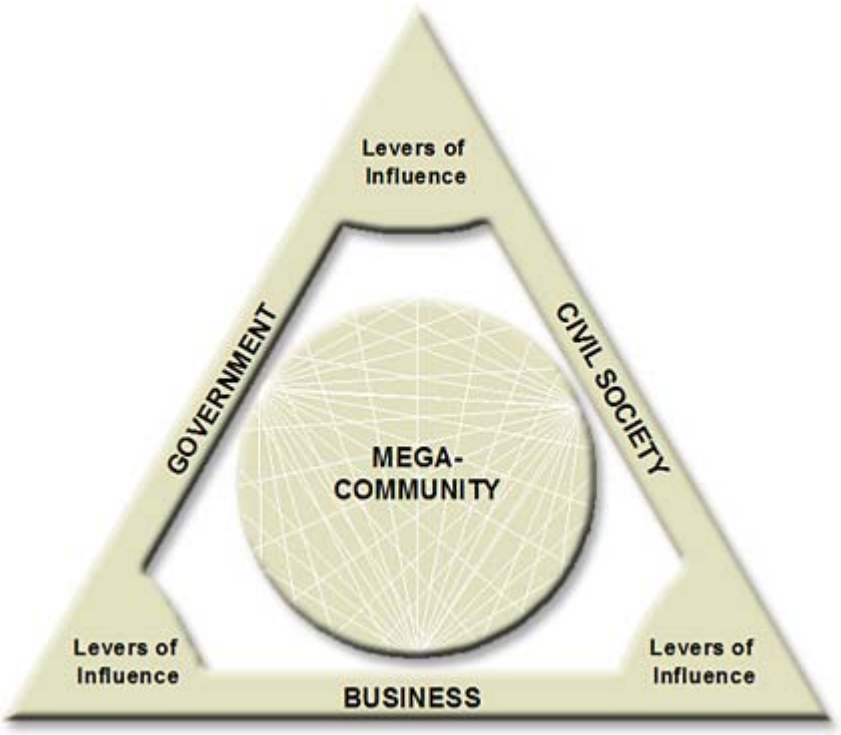


Figure 14. Mega-Community Triangle[316]

As depicted in the figure above, it is evident that no one corner of the triangle can be disconnected from the others and the responsibility for managing the

313 Gerencser, Van Lee Nepalitano and Kelly, *Megacommunities: How Leaders of Government, Business and Non-Profits Can Tackle Today's Global Challenges Together*, 55.

314 Ibid.

315 Ibid., 55-57.

316 "Megacommunity Thinking," *megacommunities.com,* http://megacommunities.com/26655021 (accessed May 12, 2008).

activities of the mega-community is vested in all three sectors.[317] As seen through this framework, the negative impact of a single sector attempting to dominate the others is evident to all and quickly creates a form of feedback that redirects the negative energy back towards the abusive sector.[318] The leaders within a mega-community are able to channel and sustain the positive natural tension through cross-sector dialogue that is not readily engaged in without the mega-community structure.[319] Building a mega-community is not an easy task and it takes a directed effort to build a successful one.

There are five essential components that define the conditions and key features necessary to build a successful mega-community: tri-sector engagement, an overlap in vital interests, convergence, cross-organizational structures, and adaptability.[320] Tri-sector engagement requires the inclusion of government, business and civil society in the mega-community structure.[321] In the case of the *Dynamic Identity Mega-Community*, this is likely to include current governmental agency stakeholders; current vendors, consultants and contractors; and civil society groups such as the American Civil Liberties Union and the Anti-Defamation League. Vital interests overlap when the sectors share and issue (security problems associated with personal identity) and when the sectors share a sense of impact created by the mutual issue (privacy versus security).[322] While the first two components are readily prevalent and identifiable in modern society, the third component, convergence, occurs only when there is more than a floating overlap of interests.[323] Convergence occurs when the separate constituencies realize that their progression towards an answer has reached a plateau or roadblock and

---

[317] Gerencser, Van Lee, Nepalitano and Kelly, *Megacommunities: How Leaders of Government, Business and Non-Profits Can Tackle Today's Global Challenges Together*, 57.

[318] Ibid.

[319] Ibid., 57-58.

[320] Ibid., 61-76.

[321] Ibid., 62-67.

[322] Ibid., 67-69.

[323] Ibid., 69.

additional efforts to solve the issue fails to achieve results.[324] This is likely the dilemma faced in the personal identity crisis we find ourselves in today.

The cross-organizational structures necessary for a mega-community are grounded in social network theory where many weak ties are more important than a limited number of strong ties.[325] In other words, while it is necessary to have a limited form of structure to a mega-community for it to survive, it is important to limit the rigidity of the structure thereby driving the integration of the three sectors to optimal levels. Finally, mega-communities are designed to be dynamic and adaptable requiring goals and objectives to be subject to change and they thrive on the principles of alignment and optimization.[326]

For a mega-community to be successful, it must embrace the concepts of optimization, sensing and awareness, and constant recalibration.[327] However, how does one start? What does it take to get a mega-community off the ground so that it can attempt to tackle the toughest problems of global proportions? This question can only be answered by those persons within the latent community that have yet to realize what it will take to solve their greatest concerns. What is known is that it takes an "Initiator" to get things started.[328] Perhaps this thesis will be the catalyst for one of its readers to become the initiator of the *Dynamic Identity Mega-Community*. An initiator is not the "Mega-Community CEO," but is the most visible leadership role within the community in its embryonic stages.[329] Initiators can come from any of the three sectors (business, civil society or government) and may, at times, be most appropriately drawn from government.[330] In any case, initiators can be defined by five attributes or conditions: they must be clear on their own vital interests; they must see the greatest value in convening a

---

[324] Gerencser, Van Lee, Nepalitano and Kelly, *Megacommunities: How Leaders of Government, Business and Non-Profits Can Tackle Today's Global Challenges Together*, 70.

[325] Ibid., 71-73.

[326] Ibid., 73-76.

[327] Ibid., 103.

[328] Ibid., 113.

[329] Ibid.

[330] Ibid., 117.

mega-community over any other approach or solution; the must have long standing/pre-existing reputations and relationships that can help get the mega-community off the ground; they must come from organizations that value innovation; and they must undertake some degree of organizational analysis before reaching out.[331] Once and initiator, an organization or individual with these attributes decides to act: both internal and external analysis must take place to ensure internal team and consensus building and external stakeholder involvement.[332] This ensures commitment of the initiating person or organization and that all of the right players are brought to the table. It also ensures that the right local interest groups are involved and protects the community against "false leaders" sent to the table to impede the process.[333] "Once a core group of initiators is established, it is up to the group to begin activating the latent mega-community."[334]

[331] Gerencser, Van Lee, Nepalitano and Kelly, *Megacommunities: How Leaders of Government, Business and Non-Profits Can Tackle Today's Global Challenges Together*, 118-122.

[332] Ibid., 123-126.

[333] Ibid., 126.

[334] Ibid., 139; *Megacommunities* provides further steps to ensure that the mega-community is structured and sustained properly. For a more in depth discussion of these attributes, see pages 143-188. For an in depth discussion of the leadership characteristics needed to sustain a Megacommunity see pages 189-217. For a Megacommunity success story, see pages 219-230.

THIS PAGE INTENTIONALLY LEFT BLANK

# IV. CONCLUSIONS AND RECOMMENDATIONS

Starting minutes after the 9/11 attacks, through the pages of the 9/11 Report and on to the theory and conceptual framework presented in the previous chapter, U.S. scholars and government officials have been focused on protecting the America's shores from the threat of Arab-Muslim terrorists for over seven years. The terrorists who wreaked havoc upon our nation that fateful day in the fall of 2001 all entered the United States legally with ambiguous name-based identities that allowed them to operate freely and undetected within our country for months before the attacks on New York and Washington. Research conducted during this project revealed that ambiguous name-based identities and their associated issues remain a major obstacle to counter-terrorism officials and that current technological solutions fail to adequately address these issues. Recent work by Hsinchun Chen noted that current research on the technologies associated with counter-terrorism lacks a consistent framework to address the major challenges.[335] Recent Presidential Directives reiterate Chen's conclusions and call for the United States Government to establish a framework to ensure "that Federal executive departments and agencies (agencies) use mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals in a lawful and appropriate manner, while respecting their information privacy and other legal rights under United States law."[336] To effectively combat terrorists and their supporters from entering or operating within the United States and to aid investigators in tracking down and defeating terrorists abroad, a new strategy must emerge that leaps beyond the current state of affairs. Such a strategy must sprint ahead of the known problem space and create a new set of rules that provides a sustainable competitive advantage in the Global War on Terror to the United States of America.

---

[335] Chen, *Intelligence and Security Informatics for International Security Information Sharing and Data Mining: Integrated Series in Information Systems*, 182.

[336] "National Security Presidential Directive 59 and Homeland Security Presidential Directive 24," *The White House*, https://www.hsdl.org/homesec/docs/whitehouse/nps36-060608-01.pdf&code=f2c9e5bec3327f27afbc9741e318ef43 (accessed August 1, 2008).

The answers to these issues lie in a strategic shift towards a view of personal name-based identity as a "dynamic" entity. The author provides his proposed solutions, *Dynamic Personal Identity* (substantive theory) and the *Dynamic Identity Grid* (conceptual framework), as the answer to Chen's questions and as a solution for the two most recent Presidential Directives. The Proposition of *Dynamic Personal Identity* is based on the kernel theories of knowledge dynamics and knowledge flow theory. These theories are based upon the principle that knowledge is a dynamic force that shares characteristics similar to those found with fluids such as inertia and flow reduction. One of the main concepts found in knowledge flow theory is that knowledge tends to clump in persons and organizations and at certain locations and times. Viewing personal name-based identity from this point of view, one can see why the current stove-piped systems and processes used by the U.S. Government are inadequate to combat the threat of global terrorism. It is highly likely that needed knowledge integral to the success of the Global War on Terror remains trapped within a Federal Government organization or within one or a few of its key personnel. The *Dynamic Identity Grid* concept presented in the previous chapter provides a starting point for the development of an overarching technological solution that will integrate Federal, State, local and maybe even foreign technological assets into a seamless personal identity mega-system ensuring personal privacy and promoting integrated knowledge management that saves both time and money while enhancing America's ability to combat global terrorism. The *Dynamic Identity Grid* is made up of five core systems from the individual user's computer to the overarching communications and technological infrastructure that drives the processes and transactions for both the human and computer users of the Grid.

Finally, the author suggests a strategy for development and implementation of the *Dynamic Identity Grid* that calls for the establishment of a *Dynamic Identity Mega-Community* to fully engage tri-sector stakeholders in the research and development process. In addition to these overarching solutions, the author calls for a standardized operational level system that consistently transliterates Arab-Muslim names; collection of the full, four-part Arab-Muslim name; the collection of certain additional characteristics of a person's identity that will promote issuance of non-ambiguous personal

identification documents based on a comprehensive *Dynamic Personal Identity*; and a variety of other transactional and analytical components within the *Dynamic Identity Grid* that will enhance U.S. efforts aimed at identifying and defeating terrorists and those who support them before they are able to strike on U.S. soil again.

It is recommended that the *Dynamic Identity Mega-Community* be tasked with making suggestions to amend current laws, rules, policies and regulations across governmental agency boundaries in order to support the unfettered development of the *Dynamic Identity Grid*. Specifically, it is recommended that the Real ID Act and policies, rules and laws related to non-immigrant visas and State issued driver licenses be amended to include the collection and storage of information necessary to transition to personal identities that are both consistent and dynamic.

Further research should be focused on development of the core systems and components necessary to make the *Dynamic Identity Grid* a reality. The most important of these core systems will be a comprehensive process system designed to consistently transliterate Arab-Muslim names from Arabic to English.

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF REFERENCES


2005 Information Sharing Guidelines.

2006 National Strategy for Combating Terrorism.

2006 National Strategy to Combat Terrorist Travel.

2007 National Strategy for Homeland Security.

2007 National Strategy for Information Sharing.

2008 U.S. Intelligence Community Information Sharing Strategy.

"About the Center for Homeland Defense and Security." *Center for Homeland Defense and Security*, https://www.chds.us/?about (accessed February 3, 2008).

"Aladdin Name Matcher – Name Matching by Normalization of Both Query and Data." *National Security Agency Central Security Service*, http://www.nsa.gov/techtrans/techt00066.cfm (accessed August 1, 2008).

"A Look at the Fort Dix Suspects." *Philadelphia Inquirer*, May 8, 2007, http://www.philly.com/philly/hp/news_update/20070508_A_look_at_the_Fort_Dix_suspects.html (accessed October 17, 2007).

Agence France-Presse, "More foreign fighters move into Pakistan's tribal areas, report," *AFP.com*, July 10, 2008, http://afp.google.com/article/ALeqM5hNzXPQQNbA3bRiC7nLUeyTyPbqSg (accessed August 1, 2008).

Al-Anzi, Fawaz S. "Stochastic Models for Automatic Diacritics Generation of Arabic Names." *Computers and the Humanities*, 38, no. 4 (2004): 469-481.

Alberts, David S. and Richard E. Hayes. *Power to the Edge: Command and Control in the Information Age*. Washington, DC: Department of Defense, 2003.

Ali, Nabil. "Parsing and Automatic Diacritization of Arabic: A Breakthrough." *Paper presented at the 13th National Computer Conference*, Riyadh, 1992.

Ansari, Hamied N. "The Islamic Militants in Egyptian Politics." *International Journal of Middle East Studies* 16, no. 1 (March 1984): 123-144.

Anti-Defamation League. "Terrorism: Al Qaeda." http://www.adl.org/terrorism/profiles/al_qaeda.asp (accessed August 1, 2008).

Apostel, Leo. "Towards the Formal Study of Models in Non-Formal Sciences." In *The Concept and Role of the Model in Mathematics and Natural and Social Sciences*. Edited by Hans Fruedenthal. Dordrecht: Reidel, 1961.

Appleton, David B. "Period Arabic Names and Naming Practices." Milpitas: The Society for Creative Anachronism, 2003, http://www.sca.org/heraldry/laurel/names/arabic-naming2.htm (accessed July 24, 2007).

Aydintasbas, Asla. "Putting it All Together." *The Opinion Journal – Wall Street Journal Online*, August 21, 2002, http://www.opinionjournal.com/editorial/feature/.html?id=110002160 (accessed August 31, 2007).

Bach, Robert. "Transforming Border Security: Prevention First." unpublished work, Naval Postgraduate School, Monterey, CA, October 2007.

Bartleby. "Dynamic - The American Heritage Dictionary." http://www.bartleby.com/61/39/D0443900.html (accessed July 12, 2008).

Basis Technology. *Transliteration Assistant.* http://www.basistech.com/transliteration-assistant/ (accessed June 1, 2007).

Beeston, A.F.L. *Arabic Nomenclature: A Summary Guide for Beginners*. Oxford: Oxford University Press, 1971.

Biometics Catalog. http://www.biometricscatalog.org/Introduction/default.aspx (accessed July 11, 2008)

Biometric Consortium. "Introduction to Biometrics." Biometric Consortium, http://www.biometrics.org/intro.htm (accessed July 11, 2008).

Biometrics. Department of the Army. Biometrics Task Force. Executive Agents for Biometrics, http://www.biometrics.dod.mil/ (accessed July 11, 2008).

Biometrics.gov. http://biometrics.gov/ (accessed July 11, 2008).

Bongar, Bruce et al. *Psychology of Terrorism*. Oxford, Oxford University Press, 2007.

Boyd, John. "OODA Loop - John Boyd." Value Based Management, http://valubasedmanagement.net/methods_boyd_ooda_loop.html (accessed June 1, 2008).

Brafman, Ori and Rod A. Beckstrom. *The Starfish and the Spider*. New York: Portfolio, 2006.

Bruner, Robert. Wayne State University. *What is Topology*. http://www.math.wayne.edu/~rrb/topology.html (accessed September 25, 2007).

Bryson, John M. *Strategic Planning for Public and Nonprofit Organizations*. San Francisco: Jossey-Bass, 2004.

Carter, Ashton B., John M. Deutch and Phillip D. Zelikow. *Catastrophic Terrorism: Elements of a National Policy*, http://www.ksg.harvard.edu/visions/publication/terrorism.htm (accessed December 4, 2007).

Chen, Hsinchun. *Intelligence and Security Informatics for International Security Information Sharing and Data Mining: Integrated Series in Information Systems*, vol. 10. New York: Springer-Verlag, 2006.

Connecticut Department of Social Services. *Privacy Issues Surrounding Personal Identification Systems*, by James Laban, 1996, www.ct.gov/dss/lib/dss/PDFs/diprivac.pdf, (accessed December 10, 2007).

Context of 1980s and 1990s: Most 9/11 Hijackers Have Middle-Class Backgrounds. See Center for Grassroots Oversight, http://www.cooperativeresearch.org/context.jsp?item=a80s90smiddleclass (accessed August 15, 2007).

Cooper, Barry. *New Political Religions*. Columbia: University of Missouri Press.

Danish Ministry of Justice. *Recruitment of Islamist Terrorists in Europe*, by Michael Taarnby, Aarhus: University of Aarhus, 2005.

Davies, Simon. Big Brother: Britain's Web of Surveillance and the New Technological Order 23. Pan 1996.

della Porta, Donatella. "Recruitment Processes in Clandestine Political Organizations. *International Social Movement Research*, 1: 155-165.

Department of Defense. *Capstone Requirements Document: Global Information Grid*. Washington, DC: USGPO, 2001.

Department of Defense. *Global Information Grid Architectural Vision*. Washington, DC: USGPO, 2007.

DeYoung, Karen. "Letter Gives Glimpse of Al Qaeda Leadership." w*ashingtonpost.com*, October 2, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/10/01/AR2006100101083.html (accessed August 1, 2008).

Eisner, Elliot W. *The Enlightened Eye: Qualitative Inquiry and the Enhancement of Educational Practice*. Upper Saddle River, NJ: Prentice, 1998.

"Epistemology Introduction." *Principa Cybernetica Web*, http://pespmc1.vub.ac.be/EPISTEMI.html (accessed February 3, 2008).

Executive Orders 12881, 13354 and 13388.

"Five Jailed for Assisting Terrorists." London Metropolitan Police Service, http://cms.met.police.uk/met/layout/set/print/content/view/full/10459 (accessed February 14, 2008).

Gania, Edwin T. *U.S. Immigration Step by Step*, 3rd Edition. Naperville: Sphinx, 2006.

Gerencser, Mark, Reginald Van Lee, Fernando Nepalitano and Christopher Kelly. *Megacommunities: How Leaders of Government, Business and Non-Profits Can Tackle Today's Global Challenges Together*. New York: Palgrave MacMillan, 2008.

Gioia, Dennis A. James B. Thomas, Shawn M. Clark, and Kumar Chittipeddi. "Symbolism and Strategic Change in Academia: The Dynamics of Sensemaking and Influence." *Organization Science*, 5, no. 3 (1994): 363-383.

Griswold v. Connecticut from Wikipedia. http://en.wikipedia.org/wiki/Griswold_v._Connecticut (accessed December 10, 2007).

Halawi, L. A and R. V. McCarthy. "Knowledge Management and the Competitive Strategy of the Firm," *The Learning Organization* 13, no. 4 (2006): 384-397.

Halpern, Jack. *Automatic Romanizer of Arabic Names – ARAN*. Tohoku: CJK Dictionary Institute, 2006, http://www.kanji.org/cjk/arabic/aran/htm (accessed August 10, 2007).

Harbinger Technologies Group. *Foxhound*, http://www.harbingertechnologiesgroup.com/technical-solutions/foxhound.html (accessed August 1, 2007).

Homeland Security Presidential Directives 2, 6, 11, 12, and 15.

Housel, Thomas J. and Arthur H. Bell. *Measuring and Managing Knowledge*. Boston: McGraw Hill, 2003.

Huxam, C. "Theorizing Collaboration Practice." *Public Management Review*, 5, no. 3, (2003): 401-423. As quoted in *Strategic Planning for Public and Nonprofit Organizations*, 378.

Ibrahim, Saad Eddin. "Anatomy of Egypt's Militant Islamic Groups." *International Journal of Middle East Studies* 12, no. 4 (December 1980): 423-453.

Ibrahim, Saad Eddin. "Egypt's Islamic Militants." *MERIP Reports* 103 (February 1982): 5-14.

Johnson, Thomas H. and M. Chris Mason. "Understanding the Taliban and Insurgency in Afghanistan." *Orbis* 51, no. 1 (Winter 2007): 71-89.

Jones, David, Michael Martin, L.R. Smith, and Mark Weeding. "Looking for the Pattern." *Studies in Conflict and Terrorism*, 26 (2003): 443-457.

Jones, Seth G. email interview with the author, August 10, 2008.

Jones, Seth G. *Getting Back on Track in Afghanistan*. Santa Monica, CA: RAND Corporation, 2008.

Jordan, Javier, Fernando Manas and Nicola Horsburgh. "Strengths and Weaknesses of Grassroots Jihadist Networks." *Studies in Conflict and Terrorism* 31, no. 1 (January 2008): 17-39.

Katzman, Kenneth. *CRS Report for Congress - Al Qaeda: Profile and Threat Assessment.* Washington, D.C.: Congressional Research Service, 2005.

Kharoba, Sam. "Understanding and Preparing for 21st Century Crime." Social Security Administration, www.ssa.gov/oig/investigations/PCIE-ECIE/presentations/**Sam_Kharoba**.pdf (accessed August 15, 2007).

Kim, W. Chan and Renee Mauborgne, *Blue Ocean Strategy*, Boston: HBS Press, 2005.

Krebs, Valdis. "Connecting the Dots." *Social Network Analysis Website*, http://orgnet.com/tnet.html (accessed January 15, 2008).

Languages of the World. *SATTS*. http://www.languages-of-the-world.us/YourNameIn/SATTS.html (accessed October 7, 2007).

Laville, Sandra and Vikram Dodd. "Widow of July 7 Attacks Ringleader Held." *The Guardian*, May 10, 2007.

Lawrence, T. E. *Seven Pillars of Wisdom*. New York, NY: Anchor, 1991.

Leedy, Paul and Jeanne Ormrod. *Practical Research: Planning and Design*. 8th Edition, New Jersey: Pearson, 2005.

Liebeskind, J. P. "Knowledge, Strategy, and the Theory of the Firm." Special Issue: Knowledge and the Firm. *Strategic Management Journal* 17 (1996): 93-107.

Lofland, John and Rodney Stark. "Becoming a World Saver: A Theory of Conversion to a Deviant Perspective." *American Sociological Review* 30, no. 6 (December 1965): 862-875.

Lutz, Richard. telephone interview with author. July 9, 2008.

Madrid Bombing Suspects. *BBC News*, http://news.bbc.co.uk/go/pr/fr/-/1/hi/world/europe/3560603.stm (accessed October 17, 2007).

Magouirk, Justin, Scott Atran and Marc Sageman. "Connecting Terrorist Networks." *Studies in Conflict and Terrorism* 31, no. 1 (January 2008): 1-16.

"Madrid Bombing Suspects." *BBC News*, http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/1/hi/world/europe/356 (accessed October 18, 2007).

"Megacommunity Thinking." *megacommunities.com,* http://megacommunities.com/26655021 (accessed May 12, 2008).

McConnell, J. Michael. *Annual Threat Assessment of the Director of National Intelligence*. Washington, DC: Office of the Director of National Intelligence, 2008.

Merriam-Webster Online. *Diacritic*. http://www.m-w.com/dictionary/diacritic (accessed September 11, 2007).

Merriam-Webster. "Biometrics." Merriam-Webster Online Dictionary, http://www.merriam-webster.com/dictionary/biometrics (accessed July 11, 2008).

Michael, James. Privacy and Human Rights 1, UNESCO 1994.

MIPT Terrorism Knowledge Base. "Al Qaeda," http://www.tkb.org/Group.jsp?GroupID=6 (accessed February 24, 2008). The Congressional Research Service estimated the group's 1998 strength at 10,000 to 20,000 members, See: Kenneth Katzman, *CRS Report for Congress - Al Qaeda: Profile and Threat Assessment* Washington D.C.: Congressional Research Service, 2005.

MIPT Terrorism Knowledge Base. "Continuity Irish Republican Army." http://www.tkb.org/Group.jsp?GroupID=37 (accessed February 24, 2008)

MIPT Terrorism Knowledge Base. "Irish Republican Army." http://www.tkb.org/Group.jsp?GroupID=55 (accessed February 24, 2008)

MIPT Terrorism Knowledge Base. "Real Irish Republican Army," http://www.tkb.org/Group.jsp?GroupID=91 (accessed February 24, 2008).

MIPT Terrorism Knowledge Base. "Al Qaeda Related Groups." http://www.tkb.org/MoreRelatedGroups.jsp?groupID=6&pageIndex=0 and http://www.tkb.org/MoreRelatedGroups.jsp?groupID=6&pageIndex=1 (accessed February 24, 2008).

MIPT Terrorism Knowledge Base. "Al Qaeda." http://www.tkb.org/Group.jsp?GroupID=6 (accessed February 24, 2008).

Murphy, Dan. "How Al Qaeda Lit the Bali Fuse." *Christian Science Monitor*, June 19, 2003.

"National Security Presidential Directive 59 and Homeland Security Presidential Directive 24." *The White House*, https://www.hsdl.org/homesec/docs/whitehouse/nps36-060608-01.pdf&code=f2c9e5bec3327f27afbc9741e318ef43 (accessed August 1, 2008).

"NGA GEOnet Names Server." *National Geospatial Intelligence Agency*, http://earth-info.nga.mil/gns/html/index.html (accessed August 1, 2008).

National Association of State Chief Information Officers. *Research Brief: Keeping Citizen Trust: What Can a State CIO Do to Protect Privacy?* www.nascio.org (accessed December 1, 2007).

National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States.* Washington, D.C.: United States Government Printing Office, 2002.

National Commission on Terrorist Attacks upon the United States. *9/11 and Terrorist Travel: Staff Report of the National Commission on Terrorist Attacks Upon the United States*, by Thomas R. Eldridge, et al. Washington, DC: Government Printing Office, 2004.

National Commission on Terrorist Attacks upon the United States. *Monograph on Terrorist Financing*, by John Roth, Douglas Greenberg and Serena Wille. Washington, DC: USGPO, 2003.

National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. Washington, D.C.: United States Government Printing Office, 2002, as applied by Robert Bach in *Transforming Border Security: Prevention Fir*st. unpublished work, Naval Postgraduate School, Monterey, CA, October 2007.

*National Geospatial Intelligence Agency*. http://www.nga.mil/portal/site/nga01/index.jsp?front_door=true (accessed August 1, 2008).

National Science and Technology Council. "Biometrics Frequently Asked Questions." http://www.biometricscatalog.org/biometrics/FAQDec2005.pdf (accessed July 11, 2008).

National Science and Technology Council. "Policy for Enabling the Development, Adoption and Use of Biometric Standards. NSTC Subcommittee on Biometrics and Identity Management." http://www.biometrics.gov/Standards/NSTC_Policy_Bio_Standards.pdf (accessed July 11, 2008).

National Science and Technology Council. "The National Biometrics Challenge." NSTC Subcommittee on Biometrics and Identity Management, http://biometrics.gov/Documents/biochallengedoc.pdf (accessed July 11, 2008).

*National Security Agency Central Security Service*. http://www.nsa.gov/research/index.cfm (accessed August 1, 2008).

National Security Presidential Directive 46.

Naval Postgraduate School. *Contextual Criticality of Knowledge-Flow Dynamics: The Tragedy of Friendly Fire*, by Mark E. Nissen, Erik Jansen, Carl Jones and Gail Thomas, Monterey, CA: Office of Naval Research, 2003.

Neuman, William L. *Social Research Methods: Qualitative and Quantitative Approaches*. Boston: Pearson, 2006.

Nielsen, B. B. "Strategic Knowledge Management Research: Tracing the Co-Evolution of Strategic Management and Knowledge Management Perspectives." *Competitiveness Review* 15, no. 1 (2005): 1-13.

Nissen, Mark E. "Dynamic Knowledge Patterns to Inform Design: A Field Study of Knowledge Stocks and Flows in an Extreme Organization." *Journal of Management and Information Science* 22, no. 3 (2006): 225-263.

Nissen. Mark E. *Harnessing Knowledge Dynamics: Principled Organizational Knowing and Learning*. Hershey: IRM Press, 2006.

Notzon, Beth and Gayle Nesom. "The Arabic Naming System." *Science Editor*, 28, no. 1 (January/February 2005): 20-21.

Pepus, Greg. KM World. *Speaking in Tongues: Foreign language KM Technologies* (July 10, 2007), http://www.kmworld.com/Articles/PrintArticle.aspx?ArticleID=36893 (accessed September 30, 2007).

Podesta, John, Peter M. Shane and Richard, C. Leone. *A Little Knowledge: Privacy, Security and Public Information after September 11.* New York: Century Foundation Press, 2004.

"Privacy and the Limits of Law." *Yale Law Journal* 89 (1980).

"Privacy as an Aspect of Human Dignity." *New York University Law Review* 971 (1964).

*Privacy and Human Rights 2002: An International Survey of Privacy Laws and Developments*, Washington, DC: Electronic Privacy Information Center (2002), 1-111.

Progressive Policy Institute. *Using Technology to Detect and Prevent Terrorism*, by Shane Ham and Robert D. Atkinson. Washington, DC, Progressive Policy Institute, 2002.

Quamus, Tim Buckwalter. *Transliteration*. http://www.qamus.org/transliteration.htm (accessed September 25, 2007).

Reeve, Simon. *The New Jackals*. Boston: Northeastern University Press, 1999.

Reynolds, Paul. "Bomber video 'points to al-Qaeda'." *BBC.com*, September 2, 2005, http://news.bbc.co.uk/2/hi/uk_news/4208250.stm (accessed August 1, 2008).

Richards, James. "Know Your Customer: Naming Conventions for Arabic, Russian, Chinese, Vietnamese, West African and Hispanic Cultures." *Oklahoma City: Bankers Online*, http://www.bankersonline.com/tools/namingconventions.pdf (accessed August 10, 2007).

Rolland, Coleen. Modeling the Requirements Engineering Process. *Information Modeling and Knowledge Bases V: The proceedings of the 3rd European-Japanese Seminar on Information Modeling and Knowledge Bases,* Held in Budapest, Hungary, May 31 – June 3, 1993, Amsterdam: ISO Press (1994): 86-97.

Rufolo, Sandra. "Have We Got A Match for You." *ChannelWeb*, October 18, 2004, http://www.crn.com/government/50500044 (accessed August 1, 2008).

Sageman, Marc. "Understanding Jihadi Networks." *Strategic Insights* IV, no. 4 (April 2005), http://www.ccc.nps.navy.mil/si/2005/Apr/sagemanApr05.asp (accessed August 1, 2008).

Sageman, Marc. *Understanding Terror Networks*. Philadelphia: UP Press, 2004.

Salih, Mahmud Husein and Yousef T. Bader. "Personal Names of Jordanian Arab Christians: A Sociocultural Study." *International Journal of Social Language,* 140 (1999): 29-43.

Schbley, Ayla Hammond. "Torn Between God, Family, and Money." *Studies in Conflict and Terrorism*, 23 (2000): 175-196.

Schimmel, Annemarie. *Islamic Names*. Edinburgh: Edinburgh University Press, 1989.

Selsky, Andrew. "Pentagon Releases Gitmo Detainees' Names." *Washington Post*, May 15, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/05/15/AR2006051500905_2.html (accessed September 1, 2007).

Senior State Department Official. Interview with author. September 1, 2007.

Senior United States Consular Official. Email interview with author. October 30, 2007.

Six Sigma. "Survey Size Calculator." http://www.isixsigma.com/offsite.asp?A=Fr&Url=http://www.surveyguy.com/SGcalc.htm (accessed December 4, 2007).

SixSigma. "How to Determine Sample Size, Determining Sample Size." http://www.isixsigma.com/library/content/c000709a.asp (accessed December 4, 2007).

Slaliba, B. and A. Al Dannan. "An Approach to Automatic Vowelization of Arabic Texts." *Paper presented at the 2nd Conference on Arabic Computation Linguistics*, Kuwait (1992).

Smith, Robert Ellis. *Ben Franklin's Website*. Sheridan Books, 2000.

Staff Writer. "A Look at the Fort Dix Suspects." *Philadelphia Inquirer*, May 8, 2007.

Stark, Rodney and William Sims Bainbridge. "Networks of Faith." *The American Journal of Sociology* 85, no. 6 (May 1980): 1376-1395.

Steiger, David M. and Natalie M. Steiger. "Decision Support as Knowledge Creation: An Information Systems Design Theory." *Proceedings of the 40th Annual Hawaii International Conference on Systems Sciences* (2007), Abstract.

Strickland, Neil. University of Sheffield Staff. *What is Topology?* http://neil-strickland.staff.shef.ac.uk/Wurble.html (accessed September 25, 2007).

Strickland, Lee S. and Jennifer Willard. "Re-Engineering the Immigration System: A Case for Data Mining and Information Assurance to Enhance Homeland Security." *Bulletin of the American Society for Information Science and Technology* 29, no. 1, (October/November 2002): 24.

Terrorist Travel Report; and Coming to America: Arab Terrorists Crossing Border, Middle Eastern Illegals Find Easy Entrance into U.S. from Mexico, by J. Zane Walley, http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=24987 (accessed December 10, 2007).

*The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*, edited by Alice Falk, 1-277. New York: Norton, 2004.

*The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*, New York: Norton, 2003.

The Boston Globe. "Pakistan tribal area called likely source of next attack on the U.S." *boston.com*, June 11, 2008, http://www.boston.com/news/world/articles/2008/06/11/pakistan_tribal_area_called_likely_source_of_next_attack_on_us/ (accessed August 1, 2008).

The International Biometric Society. "Definition of Biometrics." The International Biometric Society, http://www.biometrics.tibs.org/ (accessed July 11, 2008).

Trochim, William M. K. "Positivism and Post-Positivism." Research Methods Knowledge Base, http://www.socialresearchmethods.net/kb/positvsm.php (accessed July 12, 2008).

Trochim, William M. K. "Structure of Research." Research Methods Knowledge Base, http://www.socialresearchmethods.net/kb/strucres.php (accessed July 12, 2008).

"University and Agency Partnership Initiative." *Center for Homeland Defense and Security*, https://www.chds.us/?special/info&pgm=Partner (accessed February 3, 2008).

U.S. Department of Homeland Security. *The Terrorism Liaison Officer: A National Strategy - A Conceptual Proposal for the Office of Domestic Preparedness*, by Anthony Lukin, Date Unknown, 1.

U.S. Department of State. *Immigrant and Non-Immigrant Visas Issued at Foreign Service Posts Fiscal Years 2002-2006*, http://www.travel.state.gov/xls/FY06AnnualReport.xls (accessed November 18, 2007).

UK Government and Interpol. *A Guide to Names and Naming Practices*. Anonymous, London, UK Government Press, 2006.

United States Board of Geographic Names, *BGN Home*, http://geonames.usgs.gov/ (accessed October 7, 2007).

United States Department of Homeland Security. "Report Assessing the Impact of the Automatic Selectee and No Fly Lists," by Maureen Cooney, April 27, 2006.

United States Department of Homeland Security. *Discussions of Public Comments Received on the Automated Targeting System: System of Records Notice*, Washington, DC: US-DHS, 2006.

United States Department of Homeland Security. *US-VISIT Program, Increment 1 Privacy Impact Statement*, Washington, DC: United States Government Printing Office, 2003.

United States Department of Justice. *Privacy Policy Development Guide and Implementation Templates*, Washington, DC: United States Government Printing Office, 2006.

United States Department of State. *Foreign Affairs Manual Volume 9*. Washington, DC: United States Government Printing Office, 2008, http://www.state.gov/m/a/dir/regs/fam/c22167.htm (accessed November 18, 2007).

Viechnicki, Peter. email interview with author, July 9, 2008.

Volio, Fernando, "Legal personality, privacy and the family." In Henkin (ed.), The International Bill of Rights. Columbia University Press, 1981.

Wakefield, Jane. "Doubts over Biometric Passports." BBC.co.uk, http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/4381160.stm (accessed November 25, 2007).

Weekly Compilation of Presidential Documents. *Homeland Security Presidential Directive 11*, by The Administration of George W. Bush, http://www.gpoaccess.gov (accessed November 18, 2007).

Wellisch, Hans W. *The Conversion of Scripts: Its Nature, History and Utilization*. New York, NY: Wiley, 1978.

Wikipedia. "Translation." St. Petersburg: Wikipedia Foundation, http://en.wikipedia.org/wiki/Translation (accessed October 7, 2007).

Wurmser, David. "The Saudi Connection." *The Weekly Standard* 7, no. 7 (October 29, 2001): 15.

Zhuge, Hai. "Knowledge Flow Network Planning and Simulation." *Decision Support Systems* 42, no. 2 (November 2006): 571-592.

# INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Ms. Electra Bustle
   Florida Department of Highway Safety and Motor Vehicles
   Tallahassee, Florida

4. Colonel John Czernis
   Florida Highway Patrol
   Tallahassee, Florida

5. Major Cyrus Brown
   Florida Highway Patrol
   Orlando, Florida

6. Mr. Richard Bergin
   Naval Postgraduate School
   Monterey, California

7. Mr. Brian Steckler
   Naval Postgraduate School
   Monterey, California

8. Dr. Richard Lutz
   MITRE Corporation
   Washington, District of Columbia

9. Dr. Anders Strindberg
   Naval Postgraduate School
   Monterey, California

10. Dr. David Brannan
    Naval Postgraduate School
    Monterey, California

11. Captain Robert Simeral
    Naval Postgraduate School
    Monterey, California

12. Dr. Robert Bach
Naval Postgraduate School
Monterey, California